Unit B4

Lagrange's Theorem and small groups

Introduction

This unit rounds off this book with three separate topics.

In Section 1 you will meet *Lagrange's Theorem*, a powerful result that relates the orders of the subgroups of a group to the order of the group. You will see some simple but important corollaries of this result.

In Section 2 you will see how we can use Lagrange's Theorem, its corollaries and some other results proved earlier in this book to determine all the possible structures – that is, all the isomorphism classes – for groups of orders 1 to 7. The isomorphism classes for groups of order 8 are also described, without proof.

Section 3 is a little different from the rest of this book. It does not cover any significant new group theory, but instead gives you a chance, within the topic of group theory, to improve your skills in understanding theorems and proofs, and in producing your own proofs. These are skills that are extremely important in pure mathematics and will be needed in the rest of the module, particularly in Book E *Group theory 2* and in the analysis books (Books D and F). You will practise these skills by revisiting some of the results in group theory you have already met, and proving a few more.

1 Lagrange's Theorem

In this section you will meet one of the most important results in group theory – Lagrange's Theorem.

1.1 Orders of subgroups of a group

In Unit B2 *Subgroups and isomorphisms* we found various subgroups of the group $S(\square)$, whose non-identity elements are shown in Figure 1. In fact, we found all the subgroups of $S(\square)$, though we are not in a position to prove this at the moment. They are listed in Table 1. Remember that the **order** of a group or subgroup is the number of elements that it contains.

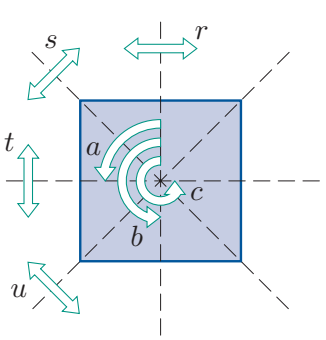


Figure 1 $S(\square)$

Table 1 The subgroups of the symmetry group $S(\square)$

Order	Number of subgroups	Subgroups
1	1	$\{e\}$
2	5	$\{e, b\}$, $\{e, r\}$, $\{e, s\}$, $\{e, t\}$, $\{e, u\}$
4	3	$\{e, a, b, c\}$, $\{e, b, r, t\}$, $\{e, b, s, u\}$
8	1	$S(\square)$

The subgroups in Table 1 are $S(\square)$ itself, all its cyclic subgroups, and two non-cyclic subgroups of order 4 that we found by modifying the square (see Subsection 1.3 of Unit B2). Notice that each of the subgroups of $S(\square)$ has an order that divides 8, the order of $S(\square)$. (An integer a is said to **divide** an integer b if a is a factor of b.) We did not find any subgroups of $S(\square)$ of orders 3, 5, 6 or 7.

Also, in Section 5 of Unit B3 *Permutations* we found all the subgroups of the symmetric group S_4. Our findings are summarised in Table 2, which is repeated from Unit B3.

Table 2 The subgroups of the symmetric group S_4

Order	Number of subgroups	Description
1	1	$\{e\}$
2	9	all cyclic
3	4	all cyclic
4	7	3 cyclic; 4 Klein
6	4	all isomorphic to $S(\triangle)$
8	3	all isomorphic to $S(\square)$
12	1	A_4
24	1	S_4

You can see from Table 2 that each subgroup of S_4 has an order that divides 24, the order of S_4.

So, for both $S(\square)$ and S_4, the order of each subgroup divides the order of the group. Lagrange's Theorem states that this is true for finite groups in general.

Theorem B68 Lagrange's Theorem

Let G be a finite group and let H be any subgroup of G. Then the order of H divides the order of G.

For example, if G is a group of order 12, then any subgroup of G has order 1, 2, 3, 4, 6 or 12. These numbers are the positive factors, also called the positive **divisors**, of 12. This group G cannot have a subgroup of order 5, 7, 8, 9, 10 or 11.

Exercise B131

Let G be a group of order n and let H be a subgroup of G. List all the possible orders of H in each of the following cases.

(a) $n = 20$ (b) $n = 25$ (c) $n = 29$

Notice that the group in the statement of Lagrange's Theorem above is referred to simply as G, without mention of its binary operation, rather than as $(G, \circ)$. It is often convenient to use this more concise notation in theorems or discussions about abstract groups, and we will do so throughout this section. This is part of a commonly used convention for notation for abstract groups that is explained more fully in the next section. (By an *abstract* group we mean one that is not a specific, concrete group such as $S(\square)$ or S_4.)

A proof of Lagrange's Theorem follows shortly. It proves the theorem by showing that if G is any finite group and H is any subgroup of G, then it is always possible to arrange the elements of G in the form of a rectangular array with the elements of H as the first row, as illustrated in Figure 2. The order of G is then the number of elements in the array, which is equal to the number of rows of the array times the number of columns of the array. Since the number of columns of the array is the order of H, it follows immediately that the order of H divides the order of G.

The proof describes a method for arranging the elements of the group G in such an array. It is helpful for you to see the method in action before you read the proof, so here is how it is carried out for the group $S(\square)$ and its 2-element subgroup $H = \langle r \rangle = \{e, r\}$. We start by writing the elements of H as the first row of the array, as follows.

$$e \quad r$$

Then we take any element of $S(\square)$ that does not appear in this row: we can choose a, for example. We compose each of the elements of H on the left with this new element to form the composite elements $a \circ e = a$ and $a \circ r = s$ (see Table 3), and write these composites below the elements of H to form a second row of the array, as follows.

$$\begin{array}{ll} e & r \\ a & s \end{array}$$

Next we take any element of $S(\square)$ that is not already in the array: we can choose b, for example. Again we compose each of the elements of H on the left with this new element to form the composite elements $b \circ e = b$ and $b \circ r = t$, and write down these composites to form a third row of the array, as follows.

$$\begin{array}{ll} e & r \\ a & s \\ b & t \end{array}$$

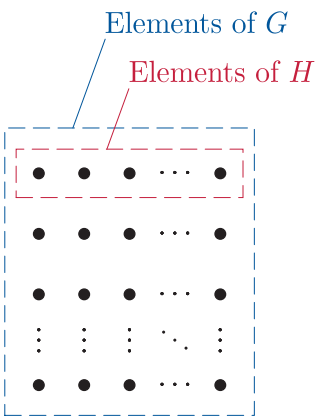


Figure 2 An arrangement of the elements of a group G with a subgroup H as the first row

Table 3 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

We continue in this way until every element of $S(\square)$ appears in the array. So next we take any element of $S(\square)$ that is not already in the array: we can choose c, for example. We compose each of the elements of H on the left with this new element to form the composite elements $c \circ e = c$ and $c \circ r = u$, and write down these composites to form a fourth row of the array, as follows.

e	r
a	s
b	t
c	u

Now every element of $S(\square)$ appears in the array, so the array is complete. It has the properties that we wanted: it is an arrangement of the elements of $S(\square)$, and it has the subgroup H as its first row.

The method that we used above must certainly produce a rectangular array of elements of $S(\square)$ with the elements of the subgroup H as the first row. However, it was not clear from the start that the array would definitely turn out to be an *arrangement of the elements of* $S(\square)$ – perhaps it was just luck that no elements of $S(\square)$ appear more than once in the array? In the proof of Lagrange's Theorem you will see that it was not just luck: the method never gives repeated elements.

You can try the method for yourself in the next exercise.

Table 4 $S(\square)$

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

Exercise B132

For each of the following subgroups of $S(\square)$, use the method demonstrated above to arrange the elements of $S(\square)$ in the form of a rectangular array whose first row consists of the elements of the subgroup. To find the necessary composites of elements of $S(\square)$, use the Cayley table of $S(\square)$, given as Table 4.

(a) $\{e, b\}$ (b) $\{e, a, b, c\}$

As mentioned earlier, it is not immediately obvious that the method demonstrated above always produces an array in which the elements are all *distinct* – and we certainly need them to be distinct so that the number of elements in the array is the order of the group that we started with. How do we know that the elements in each row will always turn out to be all different from each other, for example? And how do we know that an element obtained in one row is never repeated in another row?

The proof of Lagrange's Theorem given below describes the method demonstrated above for arranging the elements of a group G given a subgroup H, and shows that the elements of G in the resulting array are indeed always distinct. You may think the proof looks rather long, but this should not deter you from reading it: the first half of it is just the description of the method demonstrated above.

Proof of Lagrange's Theorem Let G be a finite group with binary operation $\circ$, and let H be any subgroup of G.

Let the order of H be r, and let $H = \{h_1, h_2, \ldots, h_r\}$. We form an array of elements of G by using the following procedure.

We start by writing the elements of H as the first row of the array:

$$h_1 \quad h_2 \quad \ldots \quad h_r.$$

If there are no elements of G not yet placed in the array (that is, if $H = G$), then the array is complete. Otherwise, we choose any element of G that is not yet in the array, say g_2 (the subscript 2 has been chosen for convenience, to correspond to row 2), compose each of the elements of H on the left with this new element, and write down the resulting r composites to form the second row of the array:

$$\begin{array}{cccc} h_1 & h_2 & \ldots & h_r \\ g_2 \circ h_1 & g_2 \circ h_2 & \ldots & g_2 \circ h_r. \end{array}$$

If there are no elements of G not yet placed in the array, then the array is complete. Otherwise, we choose any element of G that is not yet in the array, say g_3, compose each of the elements of H on the left with this new element, and write down the resulting r composites to form the third row of the array:

$$\begin{array}{cccc} h_1 & h_2 & \ldots & h_r \\ g_2 \circ h_1 & g_2 \circ h_2 & \ldots & g_2 \circ h_r \\ g_3 \circ h_1 & g_3 \circ h_2 & \ldots & g_3 \circ h_r. \end{array}$$

We continue appending new rows in this way until all the elements of G appear in the array. This must happen, because each new row

$$g_k \circ h_1 \quad g_k \circ h_2 \quad \ldots \quad g_k \circ h_r$$

contains the element g_k (because one of $h_1, h_2, \ldots, h_r$ is the identity element), and g_k does not appear in any previous row. So each new row includes at least one element that does not appear in any previous row.

We now show that the elements of G in the array are all distinct.

First we show that in each row of the array the r elements are all distinct. Certainly the r elements in the first row are all distinct, because they are the r elements of H. Also, the r elements in each subsequent row are all distinct, because if

$$g_k \circ h_i = g_k \circ h_j$$

for some $g_k \in G$ and $h_i, h_j \in H$, then, by the Left Cancellation Law,

$$h_i = h_j,$$

that is, h_i and h_j are the same element of H.

Next we show that none of the elements in each new row of the array is a repeat of an element that appeared in a previous row. We use a contradiction argument. Suppose that in some row, say row l, there is an element $g_l \circ h_i$ that is a repeat of an element $g_k \circ h_j$ that appeared in row k, a previous row. Then

$$g_l \circ h_i = g_k \circ h_j.$$

Composing each side of this equation on the right by h_i^{-1} gives

$$g_l = g_k \circ h_j \circ h_i^{-1}.$$

Now $h_j \circ h_i^{-1} \in H$, since H is a subgroup, so the equation above implies that the element g_l appears in row k of the array. This is a contradiction, because we chose g_l to be an element that does not appear in a previous row. Thus none of the elements in each new row of the array is a repeat of an element that appeared in a previous row. The argument here applies even if row k is the first row, since we can write the first row as

$$g_1 \circ h_1 \qquad g_1 \circ h_2 \qquad \ldots \qquad g_1 \circ h_r,$$

where $g_1 = e$.

Thus all the elements of G in the array are distinct, and hence the order of G is equal to the number of elements in the array, which is equal to the number of rows of the array times the number of columns of the array. But the number of columns of the array is r, the order of H, so the order of H divides the order of G. ■

In Book E you will see that the elements in each row of the array described in the proof above form a set known as a *left coset* of the subgroup H in the group G. Left cosets, and also right cosets, which are obtained in exactly the same way but by composing with the new elements on the right instead of the left, are hugely important in group theory, and you will learn about them, and many of their properties and uses, in Book E.

Lagrange's Theorem allows us to write down all the *possible* orders for subgroups of a finite group G – these are all the positive divisors of the order of G. Thus, if the natural number m does *not* divide the order of G, then G does not have a subgroup of order m.

Warning

The converse of Lagrange's Theorem is *false*.

Lagrange's Theorem does *not* assert that if m is a positive divisor of the order of a group G, then G has a subgroup of order m.

For example, the alternating group A_4 comprises the twelve even permutations in S_4:

$$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4), (1\ 3\ 2), (1\ 4\ 2),\\ (1\ 4\ 3), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

The group A_4 has order 12, and the positive divisors of 12 are 1, 2, 3, 4, 6 and 12, so any subgroup of A_4 must have order 1, 2, 3, 4, 6 or 12. In fact, A_4 has subgroups of each of the orders 1, 2, 3, 4 and 12, as you are asked to show in the next exercise, but it has no subgroup of order 6. You are asked to show this later in this unit, in Exercise B144 in Subsection 2.6.

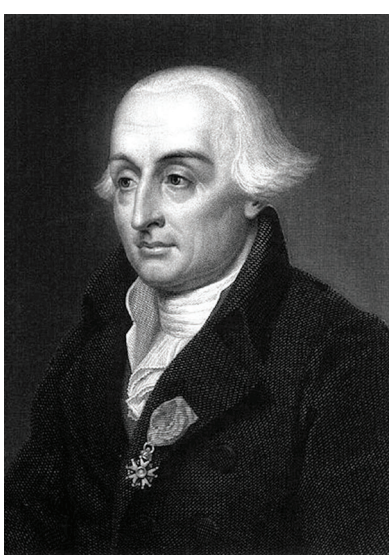
Exercise B133

Write down a subgroup of A_4 of each of the orders 1, 2, 3, 4 and 12.

Joseph-Louis Lagrange (1736–1813) was an Italian mathematician who spent his working life in Turin, Berlin and Paris. He made major contributions to mechanics, number theory and algebra. Today he is best known for his contributions to mechanics, where he transformed Newtonian mechanics into a branch of analysis, and won French Academy prizes for his work on celestial mechanics, with his memoir on the three-body problem being considered one of his most important works. (The *three-body problem* challenged mathematicians to develop a means of predicting how three neighbouring bodies in space, such as a star, a planet and a satellite, will move relative to each other.)

Lagrange's Theorem, which in modern mathematics is stated in terms of abstract groups, was obtained in the context of the theory of equations by Lagrange in 1771, a time when the concept of an abstract group had not yet been formulated. More specifically, Lagrange was trying to find an algebraic formula for the roots of a fifth degree polynomial equation and although he was unsuccessful (as Abel later showed he was bound to be), he was led to a theorem concerning the permutations of the roots of equations which, in essence, can be stated as follows: If a function of n variables is acted on by all $n!$ possible permutations of the variables and these permuted functions take only r distinct values, then r divides $n!$.

Lagrange's Theorem entered group theory with the work of both Gauss and Cauchy, each of whom proved it in particular cases. It was finally proved for any permutation group by Camille Jordan in 1861.



Joseph-Louis Lagrange (grateful acknowledgement is made to the Royal College of Physicians for the image)

1.2 Corollaries of Lagrange's Theorem

Lagrange's Theorem is a cornerstone in the theory of finite groups. We now look at some of its useful corollaries.

Orders of group elements

Remember that the **order** of an element of a finite group G is the smallest positive integer n such that $x^n = e$. From Lagrange's Theorem we can deduce the following result.

Corollary B69 to Lagrange's Theorem

Let g be an element of a finite group G. Then the order of g divides the order of G.

Proof The order of g is the same as the order of the cyclic subgroup $\langle g \rangle$ generated by g, which divides the order of G by Lagrange's Theorem. ■

For example, in the group $S(\square)$, the element a (a quarter turn anticlockwise) has order 4, which is the same as the order of the cyclic subgroup generated by a:

$$\langle a \rangle = \{e, a, a^2, a^3\} = \{e, a, b, c\}.$$

This order is a divisor of 8, the order of $S(\square)$, as guaranteed by Lagrange's Theorem.

Exercise B134

Verify that the order of the group element divides the order of the group in each of the following cases.

(a) The element (1 2 3 4) of the group S_4.

(b) The element (1 3 4) of the group S_4.

(c) The element 5 of the group $(\mathbb{Z}_9, +_9)$.

(d) The element 6 of the group $(\mathbb{Z}_9, +_9)$.

Groups of prime order

We look next at groups of prime order. Lagrange's Theorem has the following corollary.

Corollary B70 to Lagrange's Theorem

Let G be a group of prime order. Then G is cyclic, and every element of G other than the identity element is a generator of G.

Proof Let the order of the group G be the prime number p, and let x be an element of G other than the identity element. Since p is prime, it follows from Lagrange's Theorem that the cyclic subgroup $\langle x \rangle$ generated by x has order 1 or p. However, only the identity element generates a cyclic subgroup of order 1, so the order of $\langle x \rangle$ is p, and hence $\langle x \rangle$ is the whole of G. Thus G is cyclic, and x is a generator of G. ■

Note that Corollary B70 tells us in particular that if a subgroup H of a group G has prime order, then H is a cyclic subgroup of G. This is because any subgroup of a group is itself a group.

Corollary B70 also gives us the following result.

Corollary B71 to Lagrange's Theorem

If G is a group of prime order p, then G is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

Proof Let G be a group of prime order p. Then G is a cyclic group of order p, by Corollary B70. The group $(\mathbb{Z}_p, +_p)$ is also a cyclic group of order p (since $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n for any integer $n \geq 2$, by Theorem B37 in Unit B2). Any two cyclic groups of the same order are isomorphic (by Theorem B49 in Unit B2), so G is isomorphic to $(\mathbb{Z}_p, +_p)$. ■

The following corollary of Lagrange's Theorem tells us more about the structure of groups of prime order.

Corollary B72 to Lagrange's Theorem

If G is a group of prime order, then the only subgroups of G are the trivial subgroup and G itself.

Proof Let the order of G be the prime number p. Since p is prime, it follows from Lagrange's Theorem that any subgroup of G has order 1 or p. But the only subgroup of G of order 1 is the trivial subgroup $\{e\}$, and the only subgroup of G of order p is G itself. ■

An alternative way to prove Corollary B72 is to use Theorem B41 in Unit B2. This states that for any integer $n \geq 2$ the group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order q for each positive factor q of n, and no other subgroups. It follows that if p is prime, then the only subgroups of $(\mathbb{Z}_p, +_p)$ are the trivial subgroup and the whole group. By Corollary B71 (and Theorem B47 in Unit B2), the same must be true of any group of order p.

Exercise B135

Consider the group $(G, \circ)$ of order 5 that is defined by the following Cayley table.

$\circ$	v	w	x	y	z
v	w	z	y	v	x
w	z	x	v	w	y
x	y	v	z	x	w
y	v	w	x	y	z
z	x	y	w	z	v

(a) Explain how you know that G is a cyclic group.

(b) Find the identity element of G and use the Cayley table to verify that all the other elements have order 5.

(c) Find an isomorphism ϕ that maps G to $(\mathbb{Z}_5, +_5)$.

Hint: Write down a generator of G and a generator of $(\mathbb{Z}_5, +_5)$, and then find an isomorphism by matching powers of generators (as in Strategy B6, near the end of Unit B2).

Exercise B136

(a) Let G be a group of order 14. Show that all the proper subgroups of G are cyclic. (Recall that a **proper** subgroup of a group G is a subgroup that is different from G itself.)

(b) More generally, let G be a group of order pq, where p and q are both prime. Show that all the proper subgroups of G are cyclic.

Corollaries B70 and B71 to Lagrange's Theorem can sometimes help us to determine how many isomorphism classes there are for groups of a given order.

In particular, Corollary B71 tells us that for each prime number p there is just one isomorphism class for groups of order p. In other words, all groups of a particular prime order p are isomorphic to each other.

The number of isomorphism classes for groups of order n for non-prime values of n is known for small values of n. For example, there are five isomorphism classes for groups of order 8 and fourteen isomorphism classes for groups of order 16. The isomorphism classes for groups of orders 1 to 8 are described in the next section. The problem of finding the isomorphism classes for groups of order n, and how many classes there are, becomes more difficult as n increases.

2 Groups of small order

In this section we will determine how many isomorphism classes there are for groups of orders 1 to 7. That is, we will determine how many different possible structures there are for groups of these orders. We will also look at the natures of these different structures. The isomorphism classes for groups of order 8 are also described here, without proof.

2.1 Some useful results

To enable us to determine isomorphism classes for small groups, we will use several theorems that you have met in this book, together with three further, more specialised, theorems that are stated and proved in this subsection.

Before you meet these three theorems it is useful for you to be introduced to a commonly used convention for notation in group theory. You met part of this convention in the last section: you saw that we often refer to an abstract group simply as G, without mentioning its binary operation. So far, however, we have continued to denote a composite of two elements x and y of an abstract group by $x \circ y$ (as we did, for example, in the proof of Lagrange's Theorem). This notation can become unwieldy when we deal with manipulations that involve a lot of composites of group elements, so for abstract groups we often drop the use of the symbol $\circ$ in composites too. The complete convention is described below.

Notation convention for abstract groups

In discussions about abstract groups, we use the following notation and terminology where it will not cause confusion.

- We denote an abstract group simply by a single symbol such as G, without specifying a symbol for its binary operation.
- We denote a composite of two elements x and y of G simply by xy.

Warning: Unless the group is abelian, the composites xy and yx are not necessarily equal.

This convention makes the multiplicative notation that we have been using for abstract groups a little more concise. The features of multiplicative notation not mentioned in the box remain the same: for example, we continue to denote the inverse of an element x by x^{-1}, the composite of an element x with itself by x^2, the identity element by e, and so on.

The notation described in the box above, which we will refer to as *concise multiplicative notation*, will be used in discussions and proofs involving abstract groups throughout the rest of this unit, and throughout Book E, except in some circumstances where it is clearer to revert to the notation that we used previously. It is usually quicker and easier to work with, once you are used to it. When you see results stated using this notation, you need to be able to convert them into notation that involves a symbol for the binary operation, and into additive notation, so you can apply them to particular groups. The next exercise should help you become familiar with the concise multiplicative notation.

Exercise B137

(a) The following statements about elements x, y and z of a group G with identity element e are expressed using concise multiplicative notation, as described in the convention above. Write each of these statements using our previous standard notation for abstract groups, with the binary operation of G denoted by $\circ$. (One of the statements does not need to be changed.)

(i) $ex = x$ (ii) $x^2x^3 = x^5$ (iii) $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$

(iv) $x^0 = e$ (v) $xy = xz \implies y = z$

(b) Write each of the statements in part (a) in additive notation, for a group $(G, +)$.

Now here is the first of the three new theorems that we will be using to help us determine isomorphism classes in this section. Its proof is written using concise multiplicative notation.

Theorem B73

Let G be a group in which each element except the identity has order 2. Then G is abelian.

Proof Let x and y be any elements of G. We have to show that $xy = yx$. Since xy is an element of G, it is either the identity element or has order 2, and hence

$$(xy)^2 = e,$$

that is,

$$e = xyxy.$$

Composing both sides of this equation on the left with x and on the right with y gives

$$xey = x^2yxy^2,$$

and hence, since x and y are either the identity element or have order 2,

$$xey = eyxe,$$

that is,

$$xy = yx.$$

Thus G is abelian. ■

Exercise B138

Construct an alternative proof of Theorem B73 by using the fact that if a group element g is either the identity element or has order 2 then it must be self-inverse, that is, it must have the property $g = g^{-1}$. Express your proof using concise multiplicative notation.

Hint: Let x and y be elements of the group G. Start by applying the fact mentioned above to the element xy.

Now here is the second of the three theorems that we will be using to help us determine isomorphism classes.

Theorem B74

Let G be a group of order greater than 2 in which each element except the identity has order 2. Then the order of G is a multiple of 4.

Proof

We show that G has a subgroup of order 4, then apply Lagrange's Theorem.

Since G has at least three elements, we can choose two distinct non-identity elements of G, say x and y. Since x and y have order 2, we have $x^2 = e$ and $y^2 = e$, and hence $x = x^{-1}$ and $y = y^{-1}$.

Let $z = xy$. Then z is distinct from e, x and y, because every other possibility leads to a contradiction:

$z = e$ would imply $xy = e$, and hence $y = x^{-1} = x$;
$z = x$ would imply $xy = x$, and hence $y = e$;
$z = y$ would imply $xy = y$, and hence $x = e$.

We now show that $\{e, x, y, z\}$ is a subgroup of G. We start by determining the entries in the Cayley table for $\{e, x, y, z\}$. We already know that $x^2 = e$, $y^2 = e$ and $z^2 = e$, since $x, y, z \in G$. Also, by Theorem B73, the group G is abelian. Thus

$$yx = xy = z,$$
$$xz = x(xy) = x^2y = ey = y, \quad \text{so } zx = y \text{ also},$$
$$yz = y(xy) = y(yx) = y^2x = ex = x, \quad \text{so } zy = x \text{ also}.$$

Hence the Cayley table is as follows.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

We now check the three subgroup properties.

SG1 Closure Every element in the body of the table is in $\{e, x, y, z\}$, so $\{e, x, y, z\}$ is closed under the binary operation of G.

SG2 Identity The identity element e of G is in $\{e, x, y, z\}$.

SG3 Inverses All the elements of $\{e, x, y, z\}$ are self-inverse, so $\{e, x, y, z\}$ contains the inverse of each of its elements.

Thus $\{e, x, y, z\}$ is a subgroup of G. By Lagrange's Theorem, the order of this subgroup divides the order of G, so the order of G is a multiple of 4. ■

An example of a group that satisfies the conditions in Theorem B74 is $S(\square)$, the symmetry group of the rectangle, which has order 4.

The third of the three theorems in this subsection is as follows.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

Proof The elements of G that are not self-inverse can be paired up with their inverses, so G has an even number of elements that are not self-inverse. Since G has even order, it follows that G also has an even number of elements that *are* self-inverse. The identity element is a self-inverse element, so there must be at least one further self-inverse element, say x. Since $x = x^{-1}$ it follows that $x^2 = e$, so x has order 1 or 2. But x is not the identity element, so it has order 2. ■

In fact, you can see from the proof of Theorem B75 that every group of even order has an odd number of elements of order 2.

In the remaining subsections of this section we will use the three theorems above to help us determine the isomorphism classes for groups of orders 1 to 7. (The classes for groups of order 8 are also described, without proof.) We will also use Lagrange's Theorem and some of its corollaries from Section 1, and the three theorems listed below, which you met earlier in this book.

- If two finite groups are isomorphic, then they have the same order. (Theorem B43 in Unit B2.)
- All finite cyclic groups of the same order are isomorphic. (Theorem B49 in Unit B2.)
- A group of order n that contains an element of order n is a cyclic group. (Theorem B34 in Unit B2.)

2.2 Groups of orders 1, 2, 3, 5 and 7

We now make a start on determining the isomorphism classes for groups of orders 1 to 7. It is straightforward to deal with the orders 1, 2, 3, 5 and 7.

Since every group contains an identity element, a group of order 1 consists of this element alone, and hence its Cayley table is simply the following, where e is the identity element.

	e
e	e

So we can make the following observation.

Proposition B76 Isomorphism classes: order 1

There is only one isomorphism class for groups of order 1.

Examples of particular members of this isomorphism class are the groups

$$(\{0\}, +), \quad (\{1\}, \times) \quad \text{and} \quad S(F),$$

where F is any figure whose only symmetry is the identity symmetry.

Now let us consider groups of orders 2, 3, 5 and 7. All these orders are prime, so we can deal with them very easily by using Corollary B71 to Lagrange's Theorem, which states that a group of prime order p is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

Proposition B77 Isomorphism classes: orders 2, 3, 5 and 7

For each prime p, there is only one isomorphism class for groups of order p. All the groups in this class are cyclic.

For example, all groups of order 2, such as $(\mathbb{Z}_2, +_2)$, $(U_6, \times_6)$ and the group of direct symmetries of the rectangle, $S^+(\square)$, lie in the single isomorphism class for groups of order 2. That is, they are all isomorphic to each other.

Similarly, all groups of order 3, such as $(\mathbb{Z}_3, +_3)$, $(\{1, 4, 7\}, \times_9)$ and the group of direct symmetries of the triangle, $S^+(\triangle)$, lie in the single isomorphism class for groups of order 3.

Similar statements can be made for groups of orders 5 and 7.

Remember that we use the notation C_n to denote a general, abstract cyclic group of order n. So we can say that for any prime p, every group of order p is isomorphic to C_p. Remember also that every cyclic group is abelian.

2.3 Groups of order 4

In Subsection 4.2 of Unit B2 it was stated, without proof, that there are exactly two isomorphism classes for groups of order 4. We can now prove this fact.

Suppose that G is a group of order 4. By Corollary B69 to Lagrange's Theorem, the order of each element of G divides 4, so each element of G has order 1, 2 or 4. We will consider separately the following two possibilities:

- G has an element of order 4
- G has no element of order 4.

Figure 3 The pattern of the Cayley table of C_4

G has an element of order 4

If G has an element of order 4, then G is a cyclic group, isomorphic to C_4. The pattern of the Cayley table of this group is shown in Figure 3.

Examples of cyclic groups of order 4 include $(\mathbb{Z}_4, +_4)$, $(\mathbb{Z}_5^*, \times_5)$ and the group of direct symmetries of the square, $S^+(\square)$.

G has no element of order 4

Now consider the other possibility, that G does not have an element of order 4. Only the identity element has order 1, so the other three elements of G have order 2. If we let two of these elements be x and y, and we let $z = xy$, then by exactly the same argument as in the proof of Theorem B74 we can deduce that z is distinct from e, x and y, and that the Cayley table for $\{e, x, y, z\}$ is as follows.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

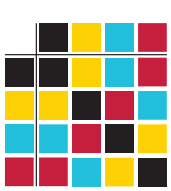


Figure 4 The pattern of the Cayley table of the Klein four-group

Since G has only four elements, this is the Cayley table of G. The table has the pattern of the Klein four-group V, shown in Figure 4, which you met in Subsection 4.2 of Unit B2. So G is isomorphic to the Klein four-group. In particular, G is abelian.

Examples of groups of order 4 isomorphic to the Klein four-group V include $(U_8, \times_8)$ and the symmetry group of the rectangle, $S(\square)$.

We have established the following result.

Proposition B78 Isomorphism classes: order 4

There are two isomorphism classes for groups of order 4:

- one contains the cyclic group C_4
- the other contains the Klein four-group V.

All groups of order 4 are abelian.

Given a group G of order 4, we can determine the isomorphism class to which it belongs by looking at the orders of its elements, as follows.

- If there are only two self-inverse elements (or, alternatively, if there is an element of order 4 – there would be two such elements), then $G \cong C_4$.
- If all elements are self-inverse (or, alternatively, if there is no element of order 4), then $G \cong V$.

Remember that the symbol $\cong$ means 'is isomorphic to'.

Recall that you can see immediately from a group table whether a particular element x is self-inverse, by checking whether the cell in the row labelled x and column labelled x contains the identity element, as illustrated in Figure 5.

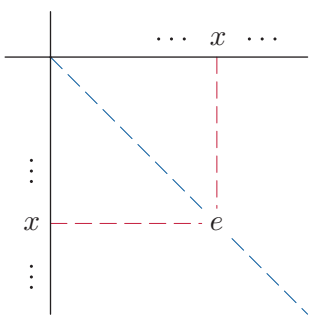


Figure 5 A self-inverse element x

Exercise B139

Each of the following sets is a subgroup of the symmetric group S_6. In each case, determine whether the subgroup is isomorphic to C_4 or to V.

(a) $\{e, (1\ 3), (2\ 5), (1\ 3)(2\ 5)\}$

(b) $\{e, (2\ 3\ 4\ 6), (2\ 4)(3\ 6), (2\ 6\ 4\ 3)\}$

Notice from the Cayley table for $\{e, x, y, z\}$ above that in a group isomorphic to the Klein four-group V, the composite of any pair of distinct non-identity elements is the third non-identity element. That is, if the three non-identity elements are x, y and z, then $xy = z$, $xz = y$ and $yz = x$. It is useful to remember this fact.

2.4 Groups of order 6

In Subsection 4.2 of Unit B2 it was stated, without proof, that there are exactly two isomorphism classes for groups of order 6. We now prove this result.

Suppose that G is a group of order 6. Then each element of G has order 1, 2, 3 or 6. We will consider separately the following two possibilities:

- G has an element of order 6
- G has no element of order 6.

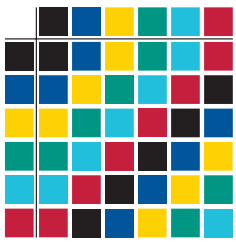


Figure 6 The pattern of the Cayley table of C_6

G has an element of order 6

If G has an element of order 6, then G is a cyclic group, isomorphic to C_6. The pattern of the Cayley table of this group is shown in Figure 6.

Examples of cyclic groups of order 6 include $(\mathbb{Z}_6, +_6)$ and $(\mathbb{Z}_7^*, \times_7)$.

G has no element of order 6

Now consider the other possibility, that G does not contain an element of order 6. In this case each non-identity element of G has order 2 or 3. By Theorem B75, since G has even order, it contains an element of order 2, say g. However, not all the non-identity elements of G have order 2, by Theorem B74, since the order of G is 6, which is not a multiple of 4. So G also contains an element of order 3, say h.

Let H be the cyclic subgroup generated by h:

$$H = \langle h \rangle = \{e, h, h^2\}.$$

The element g does not lie in H, because H has order 3 and so its elements have order 1 or 3 by Corollary B69 to Lagrange's Theorem. Hence, by the argument in the proof of Lagrange's Theorem, the following array is an arrangement of the elements of G:

$$\begin{array}{ccc} e & h & h^2 \\ g & gh & gh^2. \end{array}$$

(Remember that we are using concise multiplicative notation, so we write gh rather than $g \circ h$, and gh^2 rather than $g \circ h^2$.)

Thus the six distinct elements of G are

$$e,\ h,\ h^2,\ g,\ gh,\ gh^2.$$

We now construct a Cayley table for G. We can construct some of it directly by using the information that we have so far, as follows.

	e	h	h^2	g	gh	gh^2
e	e	h	h^2	g	gh	gh^2
h	h	h^2	e			
h^2	h^2	e	h			
g	g	gh	gh^2	e	h	h^2
gh	gh	gh^2	g			
gh^2	gh^2	g	gh			

To make further progress we need to evaluate the composite hg, which must be one of the six elements e, h, h^2, g, gh, gh^2. It cannot be h, h^2 or e since they already appear in the same row, and it cannot be g since it already appears in the same column. That leaves the possibilities gh and gh^2.

We use proof by contradiction to show that $hg \neq gh$. If $hg = gh$, then we would have

$$hg = gh \neq e,$$
$$(hg)^2 = (hg)(hg) = (hg)(gh) = hg^2h = heh = h^2 \neq e,$$
$$(hg)^3 = (hg)^2(hg) = h^2(hg) = h^3g = eg = g \neq e,$$

which would tell us that the order of hg is not 1, 2 nor 3, and hence must be 6 (since the order of a group element divides the order of the group). But this would contradict the fact that G has no element of order 6. Therefore we must have

$$hg = gh^2.$$

We can enter this in the Cayley table, and we can then fill in the rest of the top right quarter of the table using only the fact that each group element must occur exactly once in each row and each column. However, we need to calculate one more entry before we can do the same for the bottom right quarter. Since $hg = gh^2$, we have

$$(gh)g = g(hg) = g(gh^2) = g^2h^2 = eh^2 = h^2.$$

If we fill in this entry and complete the rest of the table using the fact that each group element must occur exactly once in each row and each column, then we obtain the following table.

	e	h	h^2	g	gh	gh^2
e	e	h	h^2	g	gh	gh^2
h	h	h^2	e	gh^2	g	gh
h^2	h^2	e	h	gh	gh^2	g
g	g	gh	gh^2	e	h	h^2
gh	gh	gh^2	g	h^2	e	h
gh^2	gh^2	g	gh	h	h^2	e

This table has the pattern shown in Figure 7, which is the same as the pattern of the Cayley tables of the groups $S(\triangle)$ and S_3, shown below. This pattern is not symmetric with respect to the main diagonal, so these groups are not abelian.

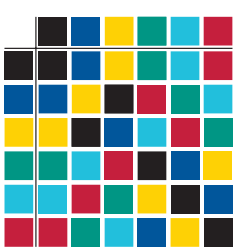


Figure 7 The pattern of the Cayley tables of $S(\triangle)$ and S_3

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

$S(\triangle)$

$\circ$	e	(123)	(132)	(23)	(13)	(12)
e	e	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	e	(12)	(23)	(13)
(132)	(132)	e	(123)	(13)	(12)	(23)
(23)	(23)	(13)	(12)	e	(123)	(132)
(13)	(13)	(12)	(23)	(132)	e	(123)
(12)	(12)	(23)	(13)	(123)	(132)	e

S_3

So we have established the following result.

Proposition B79 Isomorphism classes: order 6

There are two isomorphism classes of groups of order 6:

- one contains the cyclic group C_6
- the other contains the non-abelian group $S(\triangle)$.

Given a group G of order 6, we can determine the isomorphism class to which it belongs by using the fact that one class contains abelian groups and the other class contains non-abelian groups, as follows.

- If the group table is symmetric with respect to the main diagonal, then $G \cong C_6$.
- If the group table is not symmetric with respect to the main diagonal, then $G \cong S(\triangle)$.

Exercise B140

Find each of the following in the symmetric group S_6.

(a) A subgroup isomorphic to C_6.

(b) A subgroup isomorphic to $S(\triangle)$.

The group $S(\triangle)$ is known as the *dihedral group* of order 6.

More generally, for each integer $n \geq 3$, the symmetry group of the regular polygon with n edges is called the **dihedral group** of order $2n$. For example, $S(\square)$ is the dihedral group of order 8, $S(\pentagon)$ is the dihedral group of order 10, and so on. The dihedral group of order $2n$ is usually denoted by D_n (or, in some texts, by D_{2n}), but this notation is not used in this module.

2.5 Groups of order 8

We now turn to groups of order 8. Suppose that G is a group of order 8. Then each element of G has order 1, 2, 4 or 8. So every group of order 8 satisfies exactly one of the following three possibilities:

- G has an element of order 8
- G has no element of order 8, but has an element of order 4
- each element of G except e has order 2.

These possibilities are discussed below (in a slightly different order), with the proofs omitted.

G has an element of order 8

If G has an element of order 8, then G is a cyclic group, isomorphic to C_8. Thus G is abelian.

Such a group G comprises the identity, four elements of order 8, two elements of order 4 and one element of order 2.

An example of a cyclic group of order 8 is $(\mathbb{Z}_8, +_8)$. The orders of the elements in this group are as follows.

Element	0	1	2	3	4	5	6	7
Order	1	8	4	8	2	8	4	8

Each element of G except e has order 2

Here G is a group comprising the identity and seven elements of order 2, so, by Theorem B73, it is abelian. It can be shown that all such groups are isomorphic to each other.

An example of a group with this structure is the symmetry group of a cuboid with no square faces. You met this group in Exercise B34 in Unit B1. We can denote it by $S(\text{cuboid})$. It contains the identity symmetry, three rotations through π as shown in Figure 8, three reflections in planes halfway between opposite faces, and one further indirect symmetry, which maps each point of the cuboid to the 'opposite' point, that is, to the point that is reached if a line is drawn from the original point to the centre of the cuboid and then extended by the same distance again. You can think of this fourth indirect symmetry as 'reflection in the central point of the cuboid'.

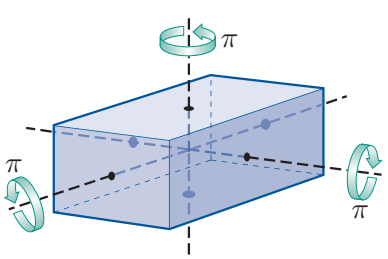


Figure 8 A cuboid and its three non-identity rotational symmetries

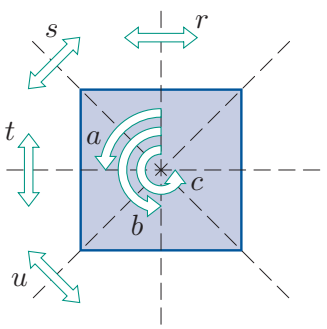


Figure 9 $S(\square)$

G has no element of order 8, but has an element of order 4

In this case, each non-identity element of G has order 2 or 4. Using an approach similar to that used for groups of order 6, we can show that there are three non-isomorphic groups of this type, as follows.

- A non-cyclic abelian group comprising the identity, four elements of order 4 and three elements of order 2. The group $(U_{15}, \times_{15})$, for example, has this structure, as you are asked to show in Exercise B141 below.
- A non-abelian group comprising the identity, two elements of order 4 and five elements of order 2. The group $S(\square)$, that is, the dihedral group of order 8, has this structure. The non-identity elements of $S(\square)$ are shown in Figure 9, and the orders of the elements are as follows.

Element	e	a	b	c	r	s	t	u
Order	1	4	2	4	2	2	2	2

- A non-abelian group comprising the identity, six elements of order 4 and one element of order 2. The standard example of such a group is the **quaternion group** of order 8, denoted by Q_8. (The blue box at the end of this subsection gives some of the history behind its name.) The elements of this group are usually denoted by

  $$1, -1, i, -i, j, -j, k, -k,$$

  where i, j and k are simply symbols, and $-i, -j$ and $-k$ denote the composites $(-1)i$, $(-1)j$ and $(-1)k$. The Cayley table for Q_8 is shown below. Notice that $i^2 = j^2 = k^2 = -1$. It is straightforward to check that the Cayley table satisfies group axioms G1 (closure), G3 (identity) and G4 (inverses), and it can be shown that it also satisfies axiom G2 (associativity).

$\times$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

The orders of the elements of Q_8 are as follows.

Element	1	-1	i	$-i$	j	$-j$	k	$-k$
Order	1	2	4	4	4	4	4	4

Exercise B141

Show that $(U_{15}, \times_{15})$ is an abelian group of order 8 that has four elements of order 4 and three elements of order 2.

Exercise B142

Use the Cayley table of the quaternion group Q_8 to show that the elements i and $-i$ of this group both have order 4.

(You can denote a composite of elements x and y of Q_8 by xy, as the binary operation of Q_8 may be thought of as a type of multiplication. Remember though that xy and yx may not be equal.)

The discussion above about groups of order 8 is summarised in the following proposition.

Proposition B80 Isomorphism classes: order 8

There are five isomorphism classes for groups of order 8, as follows.

Class	Abelian/ non-abelian	Numbers of elements of order 1	order 2	order 4	order 8	Example
1	abelian	1	1	2	4	$(\mathbb{Z}_8, +_8)$
2	abelian	1	7	0	0	$S(\text{cuboid})$
3	abelian	1	3	4	0	$(U_{15}, \times_{15})$
4	non-abelian	1	5	2	0	$S(\square)$
5	non-abelian	1	1	6	0	Q_8

This gives us the following strategy.

Strategy B14

To determine the isomorphism class of a group of order 8, determine whether the group is abelian and find the number of elements of order 2. Then use the table in Proposition B80.

You can count how many elements of order 2 there are in a finite group by looking at its Cayley table: the number of elements of order 2 is one less than the number of self-inverse elements, because the self-inverse elements are the identity element and the elements of order 2. Remember also that a finite group is abelian if and only if its Cayley table is symmetric with respect to the main diagonal.

Exercise B143

Each of the following Cayley tables is the group table of a group of order 8. In each case, use Strategy B14 to determine the isomorphism class to which the group belongs, and hence state a standard group from Proposition B80 to which the group is isomorphic.

(a)

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

(b)

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	f	g	h	e	a	b	c
f	f	g	h	d	a	b	c	e
g	g	h	d	f	b	c	e	a
h	h	d	f	g	c	e	a	b

(c)

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	d	f	g	h	e
b	b	c	d	f	g	h	e	a
c	c	d	f	g	h	e	a	b
d	d	f	g	h	e	a	b	c
f	f	g	h	e	a	b	c	d
g	g	h	e	a	b	c	d	f
h	h	e	a	b	c	d	f	g

(d)

$\circ$	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	b	a	e	c
f	f	d	h	g	c	b	a	e
g	g	f	d	h	e	c	b	a
h	h	g	f	d	a	e	c	b

William Rowan Hamilton

The quaternions

In 1834 the Irish mathematician William Rowan Hamilton (1805–1865) published a paper in which he carefully explained how complex numbers can be regarded as ordered pairs of real numbers; specifically $a + ib = (a, b)$. Complex numbers are a convenient notation for pairs, but space is three-dimensional, and his paper sparked a search for a similar notation for triples. What was required was a way of adding two triples so as to obtain a third, and multiplying two triples so as to obtain a third, in such a way that subtraction and division are also possible. The search for triples with the required properties always failed and later it was proved that no such algebra of triples can exist. But in 1843 Hamilton surprised himself by discovering an algebra of quadruples in which quadruples can be added, subtracted, multiplied and (if non-zero) divided.

Hamilton introduced three symbols i, j and k and gave them simple but unexpected rules for their multiplication:

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k, \quad jk = i, \quad ki = j,$$
$$ij = -ji, \quad jk = -kj, \quad ki = -ik.$$

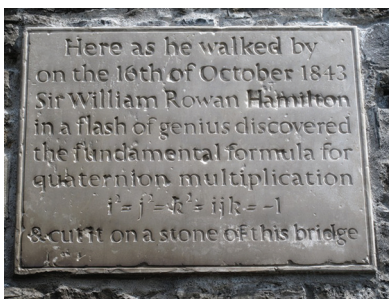
The third rule was a shock to almost everyone who saw it – everyone who had been looking for an algebra of triples up to this point had assumed that multiplication must be commutative. Hamilton then wrote quadruples as expressions of the form $w + xi + yj + zk$, where x, y, z, and w are real numbers. He called these quadruples quaternions, and studied the algebra that resulted.

Hamilton left an account of his discovery in the form of a letter to his son, Archibald, written almost twenty years later. In it he famously described how he could not 'resist the impulse – unphilosophical as it may have been – to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols, i, j, k; namely

$$i^2 = j^2 = k^2 = -1,$$

which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away.' There is now a stone plaque commemorating Hamilton's discovery set into the side of the bridge.

You saw earlier (in Subsection 3.4 of Unit B1 and Subsection 1.2 of Unit B2, respectively) that the complex numbers form an infinite group under multiplication when the element $0 = 0 + 0i$ is excluded, and $\{1, -1, i, -i\}$ is a subgroup of this infinite group. In a similar way, the quaternions form an infinite group under multiplication when the element $0 = 0 + 0i + 0j + 0k$ is excluded, and the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is a subgroup of this infinite group.



The plaque on Brougham Bridge (usually known as Broome Bridge) in Dublin. It reads: Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge

2.6 Summary of isomorphism classes for groups of orders 1 to 8

Table 5 summarises the results of Subsections 2.2 to 2.5. It lists the isomorphism classes for groups of orders 1 to 8, and places some of the groups that you have met in their classes.

Table 5 Isomorphism classes for groups of orders 1 to 8

Order	Standard group(s)	Properties	Further examples
1	C_1	cyclic	$(\{0\},+)$, $(\{1\},\times)$
2	C_2, $(\mathbb{Z}_2,+_2)$	cyclic	$S^+(\square)$, $(\mathbb{Z}_3^*,\times_3)$
3	C_3, $(\mathbb{Z}_3,+_3)$	cyclic	$S^+(\triangle)$, $(\{0,4,8\},+_{12})$, $(\{1,4,7\},\times_9)$
4	C_4, $(\mathbb{Z}_4,+_4)$	cyclic	$(\mathbb{Z}_5^*,\times_5)$, $S^+(\square)$, $S(\diamondsuit)$, $(\{0,3,6,9\},+_{12})$, $(\{1,-1,i,-i\},\times)$
	V, $S(\square)$	abelian, non-cyclic	$(U_8,\times_8)$, $(U_{12},\times_{12})$, $(\{1,7,9,15\},\times_{16})$, $(\{1,9,11,19\},\times_{20})$
5	C_5, $(\mathbb{Z}_5,+_5)$	cyclic	$S^+(\pentagon)$
6	C_6, $(\mathbb{Z}_6,+_6)$	cyclic	$S^+(\hexagon)$, $(\mathbb{Z}_7^*,\times_7)$, $(U_9,\times_9)$, $(\{0,2,4,6,8,10\},+_{12})$, $(U_{14},\times_{14})$
	$S(\triangle)$	non-abelian	S_3, $\{e,(2\,3),(2\,4),(3\,4),(2\,3\,4),(2\,4\,3)\}$
7	C_7, $(\mathbb{Z}_7,+_7)$	cyclic	S^+(heptagon)
8	C_8, $(\mathbb{Z}_8,+_8)$	cyclic	S^+(octagon)
	S(cuboid)	abelian	
	$(U_{15},\times_{15})$	abelian	$(U_{20},\times_{20})$
	$S(\square)$	non-abelian	
	Q_8	non-abelian	

In the next exercise you can use what you have learned about the isomorphism classes for small groups to show that the alternating group A_4, a group of order 12, has no subgroup of order 6, as mentioned in Subsection 1.1. This shows that although Lagrange's Theorem tells us the *possible* orders of a subgroup of a group, there may not be a subgroup of each of these possible orders.

This exercise is quite challenging: it needs puzzling out. Try it for a few minutes, and if you are not making progress then look at the hint given at the start of the solution to the exercise. (Try not to look at the solution itself when you do so!)

Exercise B144

The alternating group A_4 is given by

$$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4),\\ (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3),\\ (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Use a contradiction argument to show that A_4 has no subgroup of order 6.

3 Theorems and proofs in group theory

Throughout this book you have met many theorems and proofs, and you have been asked to produce some proofs of your own. In this section we will look again at the different ways in which theorems can be stated, in the context of the group theory that you have met, and we will revisit some of the simpler proofs in group theory that you have seen, and prove a few further results. This work should strengthen your ability to apply theorems correctly, understand proofs and produce your own proofs. These skills will be important in the remainder of the module.

3.1 Statements of theorems

Before you can prove, or indeed apply, a theorem, you need to be completely clear about what it actually claims. Any theorem can be expressed in many different ways using the elements of mathematical language that you met in Unit A3 *Mathematical language and proof*, and you will see theorems expressed in a variety of different ways throughout this module. In general, mathematicians aim to express each theorem as clearly and concisely as possible, using whatever language seems to suit that particular theorem. In this subsection you will practise interpreting theorems correctly, no matter how they are expressed.

Consider the following theorem, which you met in Unit B1. It is headed 'Proposition' rather than 'Theorem' because this word is often used for theorems that are 'less important' in some way (for example, they might be quick and straightforward to prove).

Proposition B11

In any group, the identity element is unique.

This theorem is expressed as a *universal statement*: it says that a particular property (a unique identity element) holds for *every* group. The word 'any' has been used, but it could just as well have been 'every'.

Another way in which the same theorem can be expressed is as follows.

Proposition B11 (version 2)

If G is a group, then the identity element of G is unique.

Here the theorem is stated in the form 'If P, then Q', where P and Q are statements. That is, it is expressed as an **implication**. Remember from Unit A3 that when you see a theorem expressed as an implication, it is to be interpreted as a universal statement, with the 'For all ...' part omitted but understood implicitly. For example, the statement above really means

For all G, if G is a group, then the identity element of G is unique.

Many theorems can be expressed as implications in this way.

In Unit A3 you saw that the statements P and Q in an implication 'If P then Q' are called the **hypothesis** and the **conclusion** of the implication, respectively. For Proposition B11, the hypothesis is 'G is a group' and the conclusion is 'the identity element of G is unique'.

There are various different ways to express a theorem as an implication, because, as you saw in Unit A3, an implication 'If P, then Q' can be expressed in various ways, such as those below.

Ways to express the implication 'If P, then Q'

- P implies Q
- $P \implies Q$
- P is sufficient for Q
- P only if Q
- Q whenever P
- Q follows from P
- Q is necessary for P
- Q provided that P

For instance, here are two alternative ways to express Proposition B11, by rewriting the implication in version 2 in different ways.

Proposition B11 (version 3)

The identity element of G is unique whenever G is a group.

Proposition B11 (version 4)

G is a group only if the identity element of G is unique.

Versions 3 and 4 of Proposition B11 would probably not be used in practice, because they do not read naturally and are less easy to understand than versions 1 and 2. In particular, when the phrase 'only if' appears in a theorem, it is usually part of the phrase 'if and only if', which is discussed later in this subsection.

Finally, here is one more way in which Proposition B11 can be expressed.

Proposition B11 (version 5)

Let G be a group. Then the identity element of G is unique.

Here the theorem is stated in the form 'Let P. Then Q', where P and Q are statements. This is a very common way to express a theorem that could also be expressed as an implication 'If P, then Q'. It is particularly useful when the statements P and Q are themselves quite complicated. The sentence of the form 'Let P' sets up a condition, P, that we are to assume holds for the remainder of the statement of the theorem. Then the sentence of the form 'Then Q' asserts that Q always holds under this condition. We still refer to the statements P and Q as the hypothesis and the conclusion, respectively, of the theorem. There are of course alternative ways to express the sentences of the form 'Let P' and 'Then Q': a common alternative to 'Let P' is 'Suppose P'.

Worked Exercise B48

The following theorem is from Subsection 2.2 of Unit B2. Rephrase it in the form 'If ..., then ...', and state its hypothesis and conclusion.

Theorem B29

Let x be an element of a finite group G. Then x has finite order.

Solution

The theorem can be rephrased as follows.

If x is an element of a finite group G, then x has finite order.

The hypothesis is

x is an element of a finite group G.

The conclusion is

x has finite order.

The theorem in the next exercise is headed 'Corollary'. Recall that a *corollary* is a theorem that follows from another theorem by a short additional argument.

Exercise B145

The following theorem is from Subsection 3.4 of Unit B1.

Corollary B10

If p is a prime number, then $(\mathbb{Z}_p^*, \times_p)$ is a group.

(a) State the hypothesis and conclusion of this theorem.

(b) Rephrase the theorem in each of the following forms.

(i) Let .... Then .... (ii) ... whenever ....

(iii) ... provided that .... (iv) ... only if ....

(c) Which of your answers to part (b) do you think would be good ways to state the theorem?

If the hypothesis P of a theorem is of the form 'P_1 and P_2 and ... and P_n' (it may not be phrased exactly like this, of course), then we usually call the individual statements $P_1, P_2, \ldots, P_n$ the **hypotheses** of the theorem. Similarly, if the conclusion Q is of the form 'Q_1 and Q_2 and ... and Q_n', then we usually call the individual statements $Q_1, Q_2, \ldots, Q_n$ the **conclusions** of the theorem.

No matter how a theorem is phrased, it is important that you can recognise all of its hypotheses and all of its conclusions, and that you do not mix them up. When you apply the theorem, you must make sure that all the hypotheses are satisfied before you can deduce the conclusion(s).

Worked Exercise B49

The following theorem is from Subsection 2.1 of Unit B2. (It is restated here using concise multiplicative notation.) State its hypotheses and conclusions.

Theorem B27 Index laws

Let x be an element of a group G, and let m and n be integers. The following index laws hold.

(a) $x^m x^n = x^{m+n}$

(b) $(x^m)^n = x^{mn}$

(c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

Solution

The hypotheses are

- x is an element of a group G,
- m and n are integers.

The conclusions are

- $x^m x^n = x^{m+n}$,
- $(x^m)^n = x^{mn}$,
- $(x^n)^{-1} = x^{-n} = (x^{-1})^n$.

Notice that the theorem in Worked Exercise B49 has the 'Let .... Then ....' form, but with the word 'Then' omitted and treated as understood.

Exercise B146

The following theorem is from Subsection 3.3 of Unit B2.

Theorem B37

For each integer $n \geq 2$, the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n. It is generated by the integer 1.

(a) Rewrite the theorem in the form 'If ..., then ...'.

(b) State the hypothesis (or hypotheses) and conclusion (or conclusions) of the theorem.

The next exercise asks you to state the *converse* of a theorem. Remember from Unit A3 that the **converse** of the implication 'If P then Q' is the implication 'If Q then P'. The converse of a true implication may or may not be true.

Exercise B147

The following theorem is from Subsection 3.2 of Unit B2.

Theorem B35

Every cyclic group is abelian.

(a) Rewrite the theorem in the form 'If ..., then ...'.

(You might find it helpful to introduce a symbol G for the group, as was done in version 2 of Proposition B11, discussed near the start of this subsection.)

(b) State the converse of the theorem.

(c) Is the converse true? Briefly justify your answer.

The solution to Exercise B147 illustrates another point that it is useful to keep in mind when you work with theorems and proofs. As you have seen, we aim to write mathematical statements in a way that is as clear and concise as possible. Assigning a symbol to a mathematical object may help us to do that, or it may do the opposite, or it may not make much difference either way (as is the case here). Often there are several different clear and concise ways to express a mathematical statement, and the one we use is just a matter of preference.

The next exercise asks you to try to recognise which statements from a list are correct alternative versions of a theorem from earlier in this unit. You may find it helpful to first identify the hypothesis and the conclusion of the theorem, but try also to recognise the correct versions simply by interpreting the language used in each statement in a natural way.

Exercise B148

Consider the following theorem from Subsection 2.1.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

(a) Which of the following are correct versions of this theorem?

1. Every group of even order contains an element of order 2.
2. Let G be a group that contains an element of order 2. Then G has even order.
3. A group contains an element of order 2 provided that the group has even order.
4. If G is a group of even order and $x \in G$, then x has order 2.
5. If a group contains an element of order 2, then the group has even order.
6. If G is a group of even order, then G contains an element of order 2.

(b) Which of the correct versions of the theorem from part (a) do you think are good ways to state the theorem?

(c) Which of statements 1–6 in part (a) state the converse of the theorem?

(d) Is the converse true? Briefly justify your answer.

This subsection cannot of course describe all the many different ways in which theorems can be expressed. The theorem below, from Subsection 3.4 of Unit B2, has a format that is not the same as that of any of the theorems that you have seen so far in this subsection. It starts with a sentence of the form 'Let ...'. As always, this sets up a condition that we are to assume holds for the remainder of the statement of the theorem. The theorem then asserts that a particular statement always holds under this condition. This statement is an implication.

The theorem is headed 'Lemma' rather than 'Theorem' because, as you saw in Unit A3, this word is used for theorems that are used in the proofs of other theorems.

Lemma B42

Let m be a non-zero element of the group $(\mathbb{Z}_n, +_n)$. If m is a factor of n, then m has order n/m.

In the next exercise you are asked to rephrase this theorem as an implication.

Exercise B149

(a) Rephrase Lemma B42 in the form 'If ..., then ....'. Hence state its hypothesis (or hypotheses) and conclusion (or conclusions).

(b) Which of the following are correct versions of Lemma B42?

1. If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$, then m has order n/m provided that m is a factor of n.
2. If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$ and m has order n/m, then m is a factor of n.
3. If the non-zero element m of the group $(\mathbb{Z}_n, +_n)$ is a factor of n, then it has order n/m.

The theorem below, from Subsection 3.2 of Unit B2, is expressed with a structure very like that of Lemma B42 above: it uses a sentence of the form 'Let ...' to set up a condition, then it asserts that a statement holds under this condition. However, here the statement is an *equivalence* rather than an implication.

Theorem B34

Let G be a finite group of order n. Then G is cyclic if and only if G contains an element of order n.

Remember from Unit A3 that an **equivalence** is a statement of the form 'P if and only if Q', where P and Q are statements. It asserts that *both* of the implications 'If P then Q' and 'If Q then P' hold. It can also be expressed as '$P \iff Q$', and in other ways too.

So Theorem B34 states that *both* of the following theorems hold.

Theorem B34 ('if' part)

Let G be a finite group of order n. If G contains an element of order n, then G is cyclic.

Theorem B34 ('only if' part)

Let G be a finite group of order n. If G is cyclic, then G contains an element of order n.

Exercise B150

(a) Rephrase the 'if' part of Theorem B34 in the form 'If ..., then ....'. Hence state its hypothesis (or hypotheses) and conclusion (or conclusions).

(b) Carry out part (a) for the 'only if' part.

Exercise B151

The following theorem is from Subsection 3.4 of Unit B2.

Corollary B40

Let $m \in \mathbb{Z}_n$. Then m is a generator of the group $(\mathbb{Z}_n, +_n)$ if and only if m is coprime to n.

(a) State the 'if' and the 'only if' parts of this theorem, expressing both in the form 'If ..., then ...'.

(b) State the hypothesis (or hypotheses) and conclusion (or conclusions) of the 'if' part.

(c) Carry out part (b) for the 'only if' part.

Finally in this subsection, we will revisit one more useful idea about theorems that can be written in the form 'If P, then Q', that is, $P \implies Q$. Remember from Unit A3 that the implication

$$P \implies Q$$

is equivalent to the implication

$$\text{not } Q \implies \text{not } P,$$

and that the second implication here is called the **contrapositive** of the first implication. Since an implication and its contrapositive are equivalent, saying that an implication is true is the same as saying that its contrapositive is true.

The contrapositive of a theorem provides a useful alternative interpretation of the theorem, which can be helpful when we want to apply the theorem. Also, sometimes the contrapositive of a theorem is simpler to prove than the original theorem.

Worked Exercise B50

Consider again the following theorem, from Subsection 3.2 of Unit B2. Write it in the form 'If ..., then ...', and hence write down its contrapositive.

Theorem B35

Every cyclic group is abelian.

Solution

The theorem can be written as:

If G is a cyclic group, then G is abelian.

The theorem is of the form $P \implies Q$, where

P is: G is a cyclic group,
Q is: G is abelian,
not P is: G is not a cyclic group,
not Q is: G is not abelian.

The contrapositive is:

If G is not abelian, then G is not a cyclic group.

We can state this a little more clearly.

It can also be stated as:

If a group is not abelian, then it is not cyclic.

Make sure that you do not confuse the *contrapositive* of an implication with the *converse* of an implication. Notice the difference between the contrapositive of the implication in Worked Exercise B50, and the converse of the same implication, which is

if G is an abelian group, then G is cyclic.

This converse is false, as you saw in Exercise B147.

Exercise B152

The following theorem is from Subsection 3.2 of Unit B2. Write it in the form 'If ..., then ...', and hence write down its contrapositive.

Theorem B36

Every subgroup of a cyclic group is cyclic.

3.2 Producing proofs

At first, being asked to produce a proof may feel like being asked to perform a magic trick. However, with the right support and preparation, and a good deal of practice, anyone can perform a magic trick! In the same way, learning to produce proofs requires support, preparation and practice.

There are usually two stages to producing a proof: *constructing* it, where you work out how to do it and sketch out a rough version, and *writing* it, where you explain it clearly in a form intended for someone else (or yourself at a later time) to read and understand.

Constructing a proof can be a bit like solving a puzzle: sometimes you may see immediately how to do it, but more often you will need to try out various ideas until one works. Often several different ideas will work, but some may work in a nicer – more elegant – way than others.

Usually a good approach to trying to construct a proof is to:

- write down *what you know*
- think about *what you want to prove*
- try to *bridge the gap* in an inspired way, using results and axioms that you already know.

Do not despair! Professional mathematicians regularly cover many pages with mathematics trying to find a way to prove something, and then cover even more trying to find a *nice* way to do it! Many people enjoy the challenge of doing this.

Once you think you have found a proof that works, and sketched out a rough version, you need to write it out clearly to explain it to others. You should aim to include enough explanation so that your reader does not have to rethink too much of the argument, but not so much explanation that the main argument is obscured. You should follow the usual principles of good mathematical writing: for example, you should write in sentences, use notation correctly and introduce all variables before using them. A finished proof produced by a professional mathematician, such as those given in this module, will usually have been significantly rewritten and 'polished' from the version that was first written down. Writing good proofs can be an art, one that develops with practice and reveals a little of the writer's individual style.

Sometimes, if a proof is straightforward, you may find that you can do both the constructing and the writing at the same time. Also, when you produce a proof in an examination you will not have time to polish it much, so although the logic of your proof must be correct for full marks, a lower standard of proof writing (but not a poor standard) is acceptable.

As you will have noticed, the language used in proofs is sometimes slightly different from everyday English. For example, words such as *thus*, *hence*, *therefore*, *so* and *consequently* are useful for indicating which statements follow from which. Usually you can use these words interchangeably: you may prefer to avoid repeating the same word, or you may choose a consistent wording.

The one thing that holds for all proofs is that the logical reasoning must be sound: the proof must completely justify the statement that it is proving.

Paul Erdős

Proofs from 'the Book'

The idea that mathematicians constantly strive to produce perfect proofs was evocatively captured by the prolific Hungarian mathematician Paul Erdős (1913–1996) who famously conceived of a 'transfinite Book' in which God keeps the most perfect and elegant proof of each mathematical theorem. He used the word 'transfinite' to describe the Book because, as he said, it is 'a concept in mathematics that is larger than infinite'. It has been often recounted that when Erdős was lecturing at an American summer camp to a group of highly talented students, he told them: 'You don't have to believe in God, but you should believe in the Book.'

(Source: Hoffman, P. (1998) *The Man Who Loved Only Numbers*, Hyperion, p. 26)

The next two subsections are intended to help you build up your skills with proofs by practising reading and producing proofs in group theory. You will start with some simple proofs and build up to some that are a little harder.

Throughout these subsections we will use the concise multiplicative notation for abstract groups that was introduced in Subsection 2.1. That is, we will denote a composite of two elements x and y of a general group simply by xy rather than $x \circ y$.

3.3 Proofs using the group axioms

In this subsection we will start gently by looking at how some basic properties of group elements can be deduced directly from the group axioms and from simple properties of groups that you met earlier.

Most of the results here will not be new to you; our interest here is in how they can be proved. The idea is not for you to look up and emulate the proofs of these or similar results in earlier units, but to try to prove these results afresh, find inspiration and build up your confidence in constructing proofs. The methods of proof needed are all very similar.

Here is a reminder of the group axioms, which you met in Unit B1. They are stated here using the concise multiplicative notation mentioned above.

Definition

Let G be a set on which a binary operation is defined. Then G is a **group** if the following four axioms hold.

G1 Closure For all g, h in G,

$$gh \in G.$$

G2 Associativity For all g, h, k in G,

$$g(hk) = (gh)k.$$

G3 Identity There is an element e in G such that

$$ge = g = eg \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element**.)

G4 Inverses For each element g in G, there is an element h in G such that

$$gh = e = hg.$$

(The element h is an **inverse element** of g.)

As well as using the group axioms in our proofs, we will use the first two basic properties of groups that you met in Unit B1. These are restated below; they can be proved using the group axioms, as you saw earlier, and you may assume them throughout the rest of this section.

Propositions B11 and B12

In any group,

- the identity element is unique, and we denote it by e,
- each element x has a unique inverse, which we denote by x^{-1}.

The next worked exercise demonstrates how a simple result can be proved using these properties and the group axioms.

Worked Exercise B51

Let G be a group and let x be an element of G.

Assuming only the group axioms and Propositions B11 and B12, prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

Start by writing down what we are given – the hypothesis or hypotheses. When writing out our proof, we do not need to repeat the 'Let ...' sentence in the question, even though it contains hypotheses, because any sentence of this form in a theorem or question is assumed to apply throughout the proof. (However, it is often helpful to note down such hypotheses when trying to *construct* a proof.)

Suppose that g is an element of G such that

$$gx = x.$$

We want to get to $g = e$. Both sides of the given equation end in an x, so we try composing both sides with the inverse of x.

Composing both sides of the equation on the right with the inverse of x gives

$$(gx)x^{-1} = xx^{-1}.$$

Hence

$$g(xx^{-1}) = xx^{-1} \quad \text{(by axiom G2, associativity)},$$

so

$$ge = e \quad \text{(by axiom G4, inverses)},$$

giving

$$g = e \quad \text{(by axiom G3, identity)},$$

as required.

You should usually finish a proof with some concluding words that confirm that the required result has been proved. For the simple proof in Worked Exercise B51, the final 'as required' serves this purpose.

The results in the following exercises can be proved using a method similar to that in Worked Exercise B51.

Exercise B153

Let G be a group and let a be an element of G.

Assuming only the group axioms and Propositions B11 and B12, prove that if $a^2 = a$ then $a = e$.

Exercise B154

Let G be a group, and let g and h be elements of G.

Assuming only the group axioms and Propositions B11 and B12, prove that if $gh = e$ then $h = g^{-1}$.

Note that the result in Exercise B154 is clearly true when the group G is abelian, because in that case the equation $gh = e$ is equivalent to the equation $hg = e$, giving $gh = e = hg$, which, by the definition of an inverse, implies that $h = g^{-1}$. The proof in the solution to Exercise B154 shows that the result also holds for non-abelian groups.

A more efficient way to prove the results in Worked Exercise B51 and Exercises B153 and B154 is to use the Cancellation Laws, which, as you saw in Unit B1, can be deduced from the group axioms. They are stated below, using concise multiplicative notation.

Proposition B15 Cancellation Laws

In any group G with elements a, b and x:

- if $xa = xb$, then $a = b$ (**Left Cancellation Law**)
- if $ax = bx$, then $a = b$ (**Right Cancellation Law**).

In the next worked exercise, the result in Worked Exercise B51 is proved using one of these laws. When you are trying to construct a proof, you should always consider whether you can apply results proved earlier.

Worked Exercise B52

Let G be a group and let x be an element of G.

Use one of the Cancellation Laws to prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

As usual, we start by writing down what we are given.

Let g be an element of G such that

$$gx = x.$$

We want to get to $g = e$. Both sides of the given equation end in an x, so we use the Right Cancellation Law.

By axiom G3 (identity), this equation can be written as

$$gx = ex,$$

so, by the Right Cancellation Law,

$$g = e,$$

as required.

The next two exercises ask you to repeat Exercises B153 and B154, this time using the Cancellation Laws.

Exercise B155

Let G be a group and let a be an element of G.

Use one of the Cancellation Laws to prove that if $a^2 = a$, then $a = e$.

Exercise B156

Let G be a group, and let g and h be elements of G.

Use one of the Cancellation Laws to prove that if $gh = e$, then $h = g^{-1}$.

As mentioned in Unit B1, as your familiarity with group theory grows you can start to merge some of the steps in your proofs, and not mention the group axioms every time you use them. You just need to make sure that the reasoning behind each step of your proof is either explained or will be immediately clear to a reader whose familiarity with group theory is about the same as yours. The proofs in the module texts will give you an idea of how much detail is required.

Also, you do not need to use brackets in composites of three or more group elements, since, as discussed in Unit B1, axiom G2 (associativity) tells us that the positioning of these brackets does not affect the overall composite, as long as the order of the group elements in the composite remains unchanged.

For example, here is a shorter version of the proof in Worked Exercise B51. The method is exactly the same.

Worked Exercise B53

Let G be a group and let x be an element of G.

Prove that if g is an element of G such that $gx = x$, then $g = e$.

Solution

Let $g \in G$ be such that

$$gx = x.$$

Composing both sides on the right with x^{-1} gives

$$gxx^{-1} = xx^{-1},$$

so

$$ge = e,$$

giving

$$g = e,$$

as required.

Even though brackets are not needed in composites of group elements, sometimes it can be helpful to include them, as they can make the reasoning clearer.

The results in the next two exercises can be proved using ideas similar to those that have been used in this subsection so far. You have seen Exercise B157 before, in Unit B1, but do not look back there: try it anew.

Exercise B157

Let G be a group and let a, b and c be elements of G.

Prove that if $abc = e$, then $bca = e$.

The exercise below involves the idea of two group elements *commuting*. We say that elements x and y of a group G **commute** if $xy = yx$. Thus all pairs of elements in an abelian group commute, but only some do in a non-abelian group.

Exercise B158

Let G be a group and let x and y be elements of G.

Prove that if x and y commute, then $y = xyx^{-1}$.

In the next exercise you have to try to think of a method for proving the proposition below, which is from Unit B1 and is stated here using concise multiplicative notation. You will need to think about the definition of the inverse of a group element. There is more than one way to prove this result. Do not look back at the proof provided in Unit B1!

Proposition B14

Let x and y be elements of a group G. Then

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Exercise B159

Let G be a group, and let x and y be elements of G.

Prove that $(xy)^{-1} = y^{-1}x^{-1}$.

It is important to remember Proposition B14, as it comes up frequently when we are working with group elements.

In the next exercise you will need to think about what the terms *self-inverse* and *abelian* mean, and work out a way to get from one to the other. There are different ways to do this: for example, one method involves using the group axioms, and another involves using Proposition B14.

Exercise B160

Let G be a group in which every element is self-inverse.

Prove that G is abelian.

In fact, the result in Exercise B160 is equivalent to Theorem B73 in Subsection 2.1, so you have essentially already seen a proof of it.

We end this subsection with a proof that is a little different from those in this section so far, and possibly a little tougher. It involves using *proof by induction*, which you met in Unit A3. It provides part of the proof of a result that you met in Unit B2, namely Theorem B27(c).

Remember that when you want to prove by induction that a statement $P(n)$ holds for all natural numbers n, you should proceed as follows.

1. Identify the statement $P(n)$, and state it clearly.
2. Show that $P(1)$ holds.
3. Assume that $P(k)$ holds for a general natural number k, and write down $P(k)$.
4. State that we need to deduce $P(k+1)$, and write down $P(k+1)$.
5. Deduce $P(k+1)$ from $P(k)$.
6. Conclude that $P(n)$ holds for all natural numbers n.

Exercise B161

Let G be a group and let x be an element of G.

Use mathematical induction to prove that $(x^n)^{-1} = (x^{-1})^n$ for all $n \in \mathbb{N}$.

3.4 Proofs involving subgroups

In this subsection we will look at some results about subgroups. This will provide you with further practice in reading and writing proofs. You will also meet a few results that have not appeared earlier in this book.

Here is a reminder of the definition of a subgroup, from Subsection 1.1 of Unit B2.

Definition

A **subgroup** of a group $(G, \circ)$ is a group $(H, \circ)$, where H is a subset of G.

The definition includes the symbol $\circ$ for the binary operation of the group G; it is retained here to make it clear that a subgroup of a group must have the same binary operation as the group. In this subsection, while keeping this condition in mind, we will continue to use concise multiplicative notation for abstract groups – that is, we will not use a symbol for the binary operation.

Some of the proofs in this subsection involve showing that a particular subset of a group is, or is not, a subgroup. In Unit B2 you saw that you can do this by considering three properties, called the **subgroup properties**, as stated in the following theorem.

Theorem B24 Subgroup test

Let G be a group and let H be a subset of G. Then H is a subgroup of G if and only if the following three properties hold.

SG1 Closure For all x, y in H, the composite xy is in H.

SG2 Identity The identity element e of G is in H.

SG3 Inverses For each x in H, its inverse x^{-1} is in H.

We start by proving the useful result that the intersection of any two subgroups is also a subgroup.

Worked Exercise B54

Let H and K be subgroups of a group G.

Prove that the set $H \cap K$ is a subgroup of G.

Solution

We check the three subgroup properties.

SG1 Let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$.

Use the fact that H and K are subgroups.

Since $x, y \in H$ and H is a subgroup of G, we have $xy \in H$. Likewise $xy \in K$. Hence $xy \in H \cap K$. Thus $H \cap K$ is closed.

SG2 Since H and K are subgroups of G, we have $e \in H$ and $e \in K$. Hence $e \in H \cap K$.

SG3 Let $x \in H \cap K$. Then $x \in H$ and $x \in K$.

Since $x \in H$ and H is a subgroup of G, we have $x^{-1} \in H$. Likewise $x^{-1} \in K$.

Hence $x^{-1} \in H \cap K$. Thus $H \cap K$ contains the inverse of each of its elements.

Hence $H \cap K$ satisfies the three subgroup properties, so it is a subgroup of G.

The subgroups H and K in Worked Exercise B54 are interchangeable, so when we had to prove a fact about K that we had already proved for H, we did not give the full details but instead used the word *likewise*. This

removed unnecessary detail from the proof, making it less cluttered and therefore quicker and easier to follow. Other words and phrases that can be used in place of *likewise* include *similarly* and *in a similar way*.

It is worth stating the result proved in Worked Exercise B54 as a theorem, so we can conveniently refer to it later.

Theorem B81

Let H and K be subgroups of a group G. Then $H \cap K$ is also a subgroup of G.

In the next exercise, rather than immediately launching into a proof similar to that in Worked Exercise B54, think carefully about what you know already that might be helpful.

Exercise B162

Let G be a group with subgroups H and K.

Prove that the set $H \cap K$ is a subgroup of H.

We can now say that, similarly, if H and K are subgroups of a group G, then $H \cap K$ is a subgroup of K.

We now know that intersections of subgroups are subgroups, but what about unions of subgroups?

Worked Exercise B55

Show that the following statement is false.

> If H and K are subgroups of a group G, then the set $H \cup K$ is a subgroup of G.

Solution

Remember that the statement really means the following.

> For all groups G and subgroups H and K of G, the set $H \cup K$ is a subgroup of G.

It is a *universal statement*. So to show that it is not true, we find a counterexample. We can try taking G to be a small, familiar group, and H and K to be subgroups that are easy to find, such as cyclic subgroups.

Let

$$G = S(\square) = \{e, a, r, s\},$$
$$H = \langle a \rangle = \{e, a\},$$
$$K = \langle r \rangle = \{e, r\}.$$

Then

$$H \cup K = \{e, a, r\}.$$

We need to show that this is not a subgroup. We can do this by showing that *any one* of the three subgroup properties fails. Here we can show that property SG1 (closure) fails.

Now $a, r \in H \cup K$, and

$$a \circ r = s.$$

A quick way to work out that $a \circ r = s$ is to use the fact that $S(\square)$ is isomorphic to the Klein four-group V, in which the composite of any two distinct non-identity elements is the third non-identity element (as mentioned at the end of Subsection 2.3).

However, $s \notin H \cup K$, so $H \cup K$ is not closed; that is, property SG1 fails. Hence $H \cup K$ is not a subgroup of G.

This counterexample shows that the given statement is false.

In Worked Exercise B55 we chose the group $S(\square)$ as a counterexample, but most of the other small groups that you have met would have worked just as well. Once we had chosen two subgroups of $S(\square)$, we showed that their union is not a subgroup by showing that it is not closed, but we could instead have used Lagrange's Theorem, as follows. The set $H \cup K = \{e, a, s\}$ has order 3, so by Lagrange's Theorem it cannot be a subgroup of $S(\square)$, since 3 does not divide 4.

Exercise B163

Show that the following statement is false.

> If H and K are subgroups of a group G, then the set $H \cup K$ is never a subgroup of G.

Worked Exercise B55 and Exercise B163 together show that if H and K are subgroups of a group G, then the subset $H \cup K$ may or may not be a subgroup of G.

The solution to Exercise B163 illustrates that when you are trying to find a counterexample it is often helpful to start by looking for very simple possibilities. In the next exercise finding a counterexample is not quite so straightforward.

Exercise B164

Show that the following statement is false.

> If H and K are distinct non-trivial proper subgroups of a group G, then the set $H \cup K$ is never a subgroup of G.

The next exercise asks you to prove a theorem from Unit B2. As before, try this without looking back to where the proof was first given.

Exercise B165

Prove the theorem below, using the definition that if x is an element of a group G, then $\langle x \rangle$ is the subset of G given by

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

Theorem B32

Let x be an element of a group G. Then $\langle x \rangle$ is a subgroup of G.

Here are some more exercises involving subgroups for you to try. The result in Exercise B167 is justified in Subsection 1.1 of Unit B2, but, as usual, do not look back. Exercises B168 and B169 require more thought than Exercises B166 and B167.

Exercise B166

Let H be a subgroup of a group G, and let K be a subgroup of H.

Prove that K is a subgroup of G.

Exercise B167

Prove that every subgroup of an abelian group is abelian.

Exercise B168

Let G be a group and let H and K be *distinct* subgroups of G of the same prime order.

Using Theorem B81 and Lagrange's Theorem, prove that $H \cap K = \{e\}$.

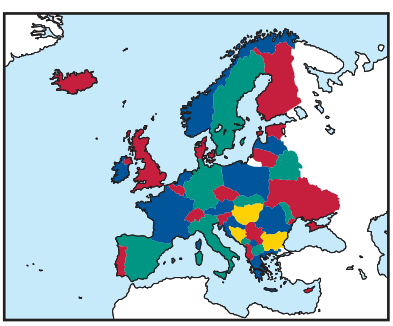
Exercise B169

Let G be a group and let H and K be subgroups of G of coprime orders.

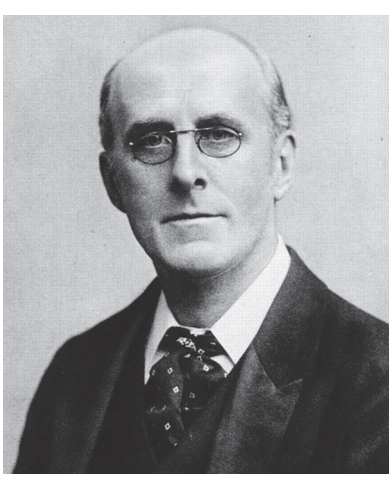
Using Theorem B81 and Lagrange's Theorem, prove that $H \cap K = \{e\}$.

3.5 Checking proofs

It is easy to make errors in proofs, so an important skill in mathematics is carefully reading mathematical arguments and spotting any problems. This is important not only for checking your own proofs, but also for checking those proposed by other people. Many people, when they do this kind of checking, tend to concentrate on the 'visible' mathematical working, such as algebraic manipulations. However, errors often lie elsewhere. For example, a logical deduction may be invalid, a definition or a theorem may have been misinterpreted, something may have been assumed that is not necessarily true, or there may be cases that have not been considered. It is important to try to look out for these sorts of problems.



A map of Europe coloured with four colours



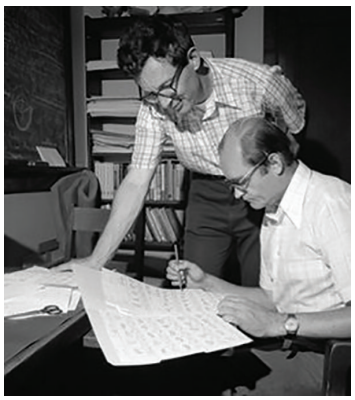
Alfred Bray Kempe

Famous errors in proofs

In 1871, the London barrister and keen mathematician Alfred Bray Kempe (1849–1922) published a 'proof' of the so-called *four-colour problem*. This problem, which asks whether every map can be coloured with at most four colours in such a way that neighbouring countries are coloured differently, had first been posed in 1852. Kempe's proof, which appeared in the newly founded *American Journal of Mathematics*, aroused considerable interest and was widely accepted. It was a very good proof – it was incorrect, but it was a very good incorrect proof! It contained sound ideas and it convinced mathematicians for 11 years until an error was found by another British mathematician, Percy John Heawood (1861–1955). The flaw in Kempe's argument turned out to be serious and, despite extensive efforts of mathematicians in Europe and in the United States, it was not until 1976 that Kenneth Appel (1932–2013) and Wolfgang Haken (1928–) found a correct proof. Their famous proof, which was several hundred pages long, had required 1000 hours of computer time. This in turn sparked a new debate: can a proof be accepted as valid if it cannot be checked by hand?

Other notable errors include one by the great French mathematician Henri Poincaré (1854–1912), who realised that he had made a crucial mistake in his original prize-winning paper of 1889 on the three-body problem. But his realisation came only after the paper had been printed and copies distributed, though fortunately before the journal in which it was due to appear had been published. Nevertheless, Poincaré had to pay for the reprinting, which cost him more than the prize he had won! Famously, it was in correcting the mistake that he discovered the foundations of what today is known as *mathematical chaos*.

A more recent example is that of Andrew Wiles' (1953–) celebrated proof of Fermat's Last Theorem. The theorem had withstood attack for over 350 years when in 1993 Wiles, after seven years of work, first presented his proof, generating a great amount of excitement. Wiles' manuscript was sent for review prior to publication and it was only then that Wiles realised there was a critical hole in his proof. A year passed and Wiles was about to give up trying to repair it when he suddenly saw how it could be done. Together with his former student Richard Taylor (1962–), Wiles repaired the hole and the 129-page proof was finally published in 1995.



Kenneth Appel (left) and Wolfgang Haken

Henri Poincaré

To check a proof, you need to read it through, very carefully, from start to finish, making sure that the correct assumptions have been used (such as the correct hypotheses), and that at each step of the argument you are convinced that each new statement does indeed follow logically from previous statements (and from other known facts). You might find it helpful to try explaining each step to yourself in different words. When you reach the end you should make sure that the correct conclusions have been reached. And you do need to check any algebraic manipulations!

If a proof uses a particular method of proof, such as proof by contradiction, proof by contraposition or proof by induction, then you need to make sure that the method has been applied correctly. In particular, for a proof by contradiction you should check that the correct negation has been used, and for a proof by contraposition you should check that the correct contrapositive has been used.

The worked exercise below contains two 'attempted proofs' of a theorem from earlier in this unit and asks whether the attempts are correct. Before you look at the solution, you might like to try checking the attempted proofs for yourself.

Andrew Wiles

Worked Exercise B56

Consider the following theorem from Subsection 2.1 of this unit.

Theorem B75

Let G be a group of even order. Then G contains an element of order 2.

Determine whether the following two attempted proofs of this theorem are correct. For each one that is incorrect, explain why.

Proof attempts (may be incorrect!)

Attempt 1
The group G has even order, so 2 divides the order of G. By Lagrange's Theorem, G has a subgroup of order 2, and such a subgroup is generated by an element of order 2. Thus G has an element of order 2.

Attempt 2
We prove the contrapositive. Let G be a group of odd order, and let g be any element of G. By Lagrange's Theorem, the order of the subgroup $\langle g \rangle$ must divide the order of G, so the order of $\langle g \rangle$ cannot be 2. Therefore g does not have order 2. Thus G does not have any elements of order 2. Since the contrapositive is true, the original statement is also true.

Solution

Attempt 1
This attempted proof is incorrect. The problem occurs in the step 'By Lagrange's Theorem, G has a subgroup of order 2'. Lagrange's Theorem tells us that the only possible orders for a subgroup of a group are the positive divisors of the order of the group, but it does not say that there *is* a subgroup of each of these possible orders.

Attempt 2
This attempted proof is also incorrect. It provides a correct proof of the following statement:

> If G is a group of odd order, then G has no element of order 2.

However, this statement is not the contrapositive of the result that is to be proved, nor is it equivalent to the result to be proved for any other reason. The correct contrapositive is as follows.

> If G is a group with no element of order 2, then G has odd order.

In fact the statement proved in Attempt 2 in Worked Exercise B56 is equivalent to the *converse* of Theorem B75.

Exercise B170

Below are four further attempted proofs of Theorem B75, the theorem stated in Worked Exercise B56.

Determine which, if any, of these attempted proofs are correct. For each one that is incorrect, explain why.

Proof attempts (may be incorrect!)

Attempt 3
The group $S(\square)$ has even order (it has order 4), and every non-identity element in $S(\square)$ has order 2. Thus a group of even order has an element of order 2.

Attempt 4
Let G be a group with an element of order 2, say g. Then $\langle g \rangle = \{e, g\}$ is a subgroup of G of order 2. By Lagrange's Theorem, since G has a subgroup of order 2, the order of G must be divisible by 2, that is, it must be even. This proves the result.

Attempt 5
Let G be a group with no element of order 2. Then every non-identity element g in G has an inverse g^{-1} that is not equal to g. These elements g and g^{-1} are inverses of each other, so every element of G, except the identity, comes in a pair. Therefore G has an odd number of elements, and so has odd order. Thus the contrapositive of the original statement is true and therefore the original statement is also true.

Attempt 6
Let G be a group of even order. We use proof by contradiction. Suppose that G does not contain an element of order 2. Then there is no element x of G that satisfies the equation $x^2 = e$. This equation is equivalent to the equation $x = x^{-1}$. However, there is an element of G that satisfies this equation, namely the identity element e, since $e = e^{-1}$. This contradiction shows that the assumption that G does not contain an element of order 2 is incorrect. Hence G does contain an element of order 2, which proves the required result.

In the final exercise in this unit you are asked to find an error in a proof and fix it.

Exercise B171

Consider the following (true) statement and attempted proof.

Statement

Let G be a finite group. Then the orders of ab and ba are the same for every a, b in G.

Proof attempt (incorrect!)

Let $a, b \in G$. Since G is finite, both ab and ba have finite order. Suppose that ab has order n. Then

$$(ab)^n = e,$$

that is,

$$\underbrace{abab\cdots ab}_{n \text{ copies of } ab} = e.$$

Composing both sides on the left with a^{-1} and on the right with a gives

$$a^{-1}a\,\underbrace{baba\cdots ba}_{n-1 \text{ copies of } ba}\,ba = a^{-1}ea,$$

that is,

$$\underbrace{baba\cdots ba}_{n \text{ copies of } ba} = e,$$

which we can write as

$$(ba)^n = e.$$

Hence ba also has order n.

Thus the orders of ab and ba are the same. This completes the proof.

(a) Contrary to the final sentence, the proof is incomplete. Explain what the problem is.

Hint: Think carefully about the definition of the order of a group element.

(b) Provide the missing portion of the proof.

Summary

In this unit you have met Lagrange's Theorem, one of the most fundamental theorems in group theory. You have seen how by using this theorem together with other theorems from earlier in this book we can determine the different isomorphism classes for groups of orders 1 to 7, and you have met the isomorphism classes for groups of order 8. You have also practised working with theorems and proofs, which are crucial components of pure mathematics. Now that you have reached this point, you should be starting to appreciate the beauty of group theory, and the power of the type of abstract approach that it exemplifies. You should be ready to go on to the deeper group theory presented in Book E.

Learning outcomes

After studying this unit, you should be able to:

- understand and apply Lagrange's Theorem and its corollaries
- understand the structure of all groups of prime order
- describe the isomorphism classes for groups of orders 1 to 8
- determine the isomorphism class to which a given group of order 8 or less belongs
- understand and apply theorems expressed in a variety of different ways
- read and understand simple proofs in group theory
- prove simple results in group theory
- check simple proofs.

Solutions to exercises

Solution to Exercise B131

It follows from Lagrange's Theorem (Theorem B68) that in each case the possible orders of the subgroups are the positive divisors of n.

(a) The possible orders are 1, 2, 4, 5, 10 and 20.

(b) The possible orders are 1, 5 and 25.

(c) The possible orders are 1 and 29.

Solution to Exercise B132

In each case there are several possibilities for the array, depending on which element we choose each time there is a choice to be made. If we always choose the first possible element from the list e, a, b, c, r, s, t, u, then we obtain the following arrays.

(a)
$$\begin{array}{cc} e & b \\ a & c \\ r & t \\ s & u \end{array}$$

(b)
$$\begin{array}{cccc} e & a & b & c \\ r & u & t & s \end{array}$$

Solution to Exercise B133

The table below contains a complete list of all the subgroups of A_4 together with their orders.

Order	Subgroup of A_4
1	$\{e\}$
2	$\{e, (1\ 2)(3\ 4)\}$
2	$\{e, (1\ 3)(2\ 4)\}$
2	$\{e, (1\ 4)(2\ 3)\}$
3	$\langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$
3	$\langle(1\ 2\ 4)\rangle = \langle(1\ 4\ 2)\rangle = \{e, (1\ 2\ 4), (1\ 4\ 2)\}$
3	$\langle(1\ 3\ 4)\rangle = \langle(1\ 4\ 3)\rangle = \{e, (1\ 3\ 4), (1\ 4\ 3)\}$
3	$\langle(2\ 3\ 4)\rangle = \langle(2\ 4\ 3)\rangle = \{e, (2\ 3\ 4), (2\ 4\ 3)\}$
4	$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$
12	A_4

All the subgroups of A_4, except the one of order 4 and A_4 itself, are cyclic subgroups. The subgroup of order 4 represents the symmetry group of the labelled rectangle below.

Solution to Exercise B134

(a) The order of S_4 is $4! = 24$.

The permutation (1 2 3 4) is a 4-cycle and so has order 4.

Hence the order of (1 2 3 4) divides the order of S_4.

(b) As in part (a), the order of S_4 is $4! = 24$.

The permutation (1 3 4) is a 3-cycle and so has order 3.

Hence the order of (1 3 4) divides the order of S_4.

(c) The order of $(\mathbb{Z}_9, +_9)$ is 9.

The consecutive multiples of 5 in $(\mathbb{Z}_9, +_9)$ are

$$\ldots, 0, 5, 1, 6, 2, 7, 3, 8, 4, 0, \ldots,$$

so the order of 5 in $(\mathbb{Z}_9, +)$ is 9.

Hence the order of 5 divides the order of $(\mathbb{Z}_9, +_9)$.

(d) As in part (c), the order of $(\mathbb{Z}_9, +_9)$ is 9.

The consecutive multiples of 6 in $(\mathbb{Z}_9, +_9)$ are

$$\ldots, 0, 6, 3, 0 \ldots,$$

so the order of 6 in $(\mathbb{Z}_9, +)$ is 3.

Hence the order of 6 divides the order of $(\mathbb{Z}_9, +_9)$.

Solution to Exercise B135

(a) The group G has order 5, which is a prime number, so G is cyclic, by Corollary B70.

(b) The identity element in the group is y, because the row and column labelled y repeat the borders of the table.

To verify that the other elements have order 5, we calculate their successive powers, using the information in the Cayley table. We have

$$v^2 = v \circ v = w,$$
$$v^3 = v^2 \circ v = w \circ v = z,$$
$$v^4 = v^3 \circ v = z \circ v = x,$$
$$v^5 = v^4 \circ v = x \circ v = y,$$

so v has order 5. Similarly,

$$w^2 = w \circ w = x,$$
$$w^3 = w^2 \circ w = x \circ w = v,$$
$$w^4 = w^3 \circ w = v \circ w = z,$$
$$w^5 = w^4 \circ w = z \circ w = y,$$

so w has order 5;

$$x^2 = x \circ x = z,$$
$$x^3 = x^2 \circ x = z \circ x = w,$$
$$x^4 = x^3 \circ x = w \circ x = v,$$
$$x^5 = x^4 \circ x = v \circ x = y,$$

so x has order 5;

$$z^2 = z \circ z = v,$$
$$z^3 = z^2 \circ z = v \circ z = x,$$
$$z^4 = z^3 \circ z = x \circ z = w,$$
$$z^5 = z^4 \circ z = w \circ z = y,$$

so z has order 5.

(c) The group G has generators w, x, v and z.

The group $(\mathbb{Z}_5, +_5)$ has generators 1, 2, 3 and 4.

Using the technique of matching powers of the generators w and 1, we obtain the following isomorphism.

$$\begin{aligned} \phi : G &\longrightarrow \mathbb{Z}_5 \\ y &\longmapsto 0 \\ w &\longmapsto 1 \\ w \circ w &\longmapsto 1 +_5 1 \\ w \circ w \circ w &\longmapsto 1 +_5 1 +_5 1 \\ w \circ w \circ w \circ w &\longmapsto 1 +_5 1 +_5 1 +_5 1 \end{aligned}$$

This simplifies to the following.

$$\begin{aligned} \phi : G &\longrightarrow \mathbb{Z}_5 \\ y &\longmapsto 0 \\ w &\longmapsto 1 \\ x &\longmapsto 2 \\ v &\longmapsto 3 \\ z &\longmapsto 4 \end{aligned}$$

(There are three other isomorphisms, obtained from $w \longmapsto 2$, $w \longmapsto 3$ and $w \longmapsto 4$.)

Solution to Exercise B136

(a) Since $|G| = 14$, the possible orders of proper subgroups of G are 1, 2 and 7, by Lagrange's Theorem.

The trivial subgroup has order 1, so is certainly cyclic. Also, since 2 and 7 are primes, any subgroup of G of order 2 or 7 is cyclic, by Corollary B70 to Lagrange's Theorem.

Thus every proper subgroup of G is cyclic.

(b) We generalise the argument in part (a). Since $|G| = pq$, where both p and q are primes, the possible orders of proper subgroups of G are 1, p and q, by Lagrange's Theorem.

The trivial subgroup has order 1, so is certainly cyclic. Also, since p and q are primes, any subgroup of G of order p or q is cyclic, by Corollary B70 to Lagrange's Theorem.

Thus every proper subgroup of G is cyclic.

Solution to Exercise B137

(a) **(i)** The statement $ex = x$ is rewritten as

$$e \circ x = x.$$

(ii) The statement $x^2x^3 = x^5$ is rewritten as

$$x^2 \circ x^3 = x^5.$$

(iii) The statement $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$ is rewritten as

$$(x \circ y \circ z)^{-1} = z^{-1} \circ y^{-1} \circ x^{-1}.$$

(iv) The statement $x^0 = e$ does not need to be rewritten.

(v) The statement $xy = xz \implies y = z$ is rewritten as

$$x \circ y = x \circ z \implies y = z.$$

(b) (i) The statement $ex = x$ is rewritten as

$$0 + x = x.$$

(ii) The statement $x^2x^3 = x^5$ is rewritten as

$$2x + 3x = 5x.$$

(iii) The statement $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$ is rewritten as

$$-(x + y + z) = (-z) + (-y) + (-x),$$

or, since every additive group is abelian,

$$-(x + y + z) = (-x) + (-y) + (-z).$$

(iv) The statement $x^0 = e$ is rewritten as

$$0x = 0.$$

(v) The statement $xy = xz \implies y = z$ is rewritten as

$$x + y = x + z \implies y = z.$$

Solution to Exercise B138

Let G be a group in which each element except the identity has order 2, and let x and y be elements of G. We have to show that $xy = yx$. Since $xy \in G$ and since $g = g^{-1}$ for each $g \in G$, we have

$$\begin{aligned} xy &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &= yx. \end{aligned}$$

Thus G is abelian.

Solution to Exercise B139

(a) The orders of the elements are as follows.

Element	e	$(1\ 3)$	$(2\ 5)$	$(1\ 3)(2\ 5)$
Order	1	2	2	2

Since the group contains no element of order 4, it is isomorphic to V.

(b) The orders of the elements are as follows.

Element	e	$(2\ 3\ 4\ 6)$	$(2\ 4)(3\ 6)$	$(2\ 6\ 4\ 3)$
Order	1	4	2	4

Since the group contains an element of order 4, it is isomorphic to C_4.

(The group in part (b) is the cyclic subgroup generated by $(2\ 3\ 4\ 6)$ or by $(2\ 6\ 4\ 3)$.)

Solution to Exercise B140

There are many possible answers.

(a) Any cyclic subgroup of S_6 of order 6 is isomorphic to C_6. One possibility is the subgroup generated by the permutation $(1\ 2\ 3\ 4\ 5\ 6)$:

$$\begin{aligned} &\langle (1\ 2\ 3\ 4\ 5\ 6) \rangle \\ &= \{e,\ (1\ 2\ 3\ 4\ 5\ 6),\ (1\ 3\ 5)(2\ 4\ 6), \\ &\quad (1\ 4)(2\ 5)(3\ 6),\ (1\ 5\ 3)(2\ 6\ 4),\ (1\ 6\ 5\ 4\ 3\ 2)\}. \end{aligned}$$

(b) Any non-abelian subgroup of S_6 of order 6 is isomorphic to $S(\triangle)$. One possibility is the subgroup

$$\{e,\ (2\ 3),\ (2\ 6),\ (3\ 6),\ (2\ 3\ 6),\ (2\ 6\ 3)\}$$

obtained by labelling the vertices of the equilateral triangle with the symbols 2, 3 and 6.

Solution to Exercise B141

We know that $(U_{15}, \times_{15})$ is a group, by Theorem B9 in Unit B1. It is abelian, since $\times_{15}$ is a commutative binary operation.

We have

$$U_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\},$$

so $(U_{15}, \times_{15})$ has order 8.

The identity element 1 has order 1.

The consecutive powers of 2 in $(U_{15}, \times_{15})$ are

$$\ldots, 1, 2, 4, 8, 1, 2, 4, 8, \ldots,$$

so 2 has order 4. The element immediately before the identity element 1 in the cycle of powers of 2 is 8, so 8 is the inverse of 2 and hence it also has order 4. Also, the cycle above shows that the consecutive powers of $4 = 2^2$ are

$$\ldots, 1, 4, 1, 4, 1, 4 \ldots,$$

so 4 has order 2.

The consecutive powers of 7 are

$$\ldots, 1, 7, 4, 13, 1, 7, 4, 13, \ldots,$$

So 7 has order 4, and 13, the inverse of 7, also has order 4.

The consecutive powers of 11 are

$$\ldots, 1, 11, 1, 11, \ldots.$$

So 11 has order 2.

The consecutive powers of 14 are

$$\ldots, 1, 14, 1, 14, \ldots.$$

So 14 has order 2.

In summary, the orders of the elements of $(U_{15}, \times_{15})$ are as follows.

Element	1	2	4	7	8	11	13	14
Order	1	4	2	4	4	2	4	2

So $(U_{15}, \times_{15})$ is an abelian group of order 8 that has four elements of order 4 and three elements of order 2.

(When you are carrying out calculations in modular arithmetic like those above, remember that there are ways to make your calculations quicker and easier, as you saw in Unit A2 *Number systems*. For example, to work out 14^2 in $(U_{15}, \times_{15})$, instead of starting by working out $14^2 = 196$, you can proceed as follows:

$$14^2 \equiv 14 \times 14 \equiv (-1) \times (-1) \equiv 1 \pmod{15}.$$

Thus $14 \times_{15} 14 = 1$.)

Solution to Exercise B142

The Cayley table for Q_8 shows that the identity element of Q_8 is 1. Also, by the Cayley table, we have

$$i^2 = -1,$$
$$i^3 = i^2 i = (-1)i = -i,$$
$$i^4 = i^3 i = (-i)i = 1,$$

and

$$(-i)^2 = -1,$$
$$(-i)^3 = (-i)^2(-i) = (-1)(-i) = i,$$
$$(-i)^4 = (-i)^3(-i) = i(-i) = 1.$$

Thus i and $-i$ both have order 4.

Solution to Exercise B143

(a) This group is abelian and has 7 elements of order 2, so it belongs to class 2. It is isomorphic to $S(\text{cuboid})$.

(b) This group is abelian and has exactly 3 elements of order 2, so it belongs to class 3. It is isomorphic to $(U_{15}, \times_{15})$.

(c) This group is abelian and has only one element of order 2, so it belongs to class 1. It is isomorphic to $(\mathbb{Z}_8, +_8)$.

(Note also the bottom left to top right diagonal stripe pattern of the Cayley table: this shows that this group is cyclic.)

(d) This group is non-abelian and has only one element of order 2, so it belongs to class 5. It is isomorphic to the quaternion group Q_8.

Solution to Exercise B144

(Hint for finding a solution to this exercise: Assume that A_4 has a subgroup H of order 6. By considering isomorphism classes, determine what the orders of the elements of H must be. Then show that H has a subgroup whose order does not divide 6.)

Suppose that A_4 has a subgroup H of order 6.

As A_4 has no element of order 6, H is isomorphic to the non-abelian group $S(\triangle)$. Thus H contains e, two elements of order 3 and three elements of order 2.

Now A_4 contains only three elements of order 2, namely

$$(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),$$

so these must all be in H. However, these three elements of order 2, along with e, form a subgroup of S_4 (it is the subgroup obtained by labelling the vertices of the rectangle with the symbols 1, 2, 3 and 4). This subgroup is a subgroup of H.

This subgroup has order 4, which contradicts Lagrange's Theorem, as 4 does not divide 6.

Thus A_4 has no subgroup of order 6.

(Here is an alternative solution, which you might have found. It starts in the same way as the solution above.

Suppose that A_4 has a subgroup H of order 6.

As A_4 has no element of order 6, H is isomorphic to the non-abelian group $S(\triangle)$. Thus H

contains e, two elements of order 3 and three elements of order 2.

Now A_4 contains only three elements of order 2, namely

$$(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),$$

so these must all be in H. Also, the two elements of order 3 in H must be inverses of each other, so they must be

$$(a\ b\ c) \quad \text{and} \quad (a\ c\ b),$$

for some distinct $a, b, c \in \{1, 2, 3, 4\}$. Let d be the element of $\{1, 2, 3, 4\}$ other than a, b and c. Then the permutation $(a\ b)(c\ d)$ is an element of H, since H contains all three possible permutations of this form. Thus, since H is a subgroup, the composite

$$(a\ b\ c) \circ (a\ b)(c\ d) = (a\ c\ d)$$

is also an element of H. This contradicts the fact that the only elements of order 3 in H are $(a\ b\ c)$ and $(a\ c\ b)$.

Thus A_4 has no subgroup of order 6.)

Solution to Exercise B145

(a) The hypothesis is

p is a prime number.

The conclusion is

$(\mathbb{Z}_p^*, \times_p)$ is a group.

(b) The theorem can be rephrased in the following forms.

(i) Let p be a prime number. Then $(\mathbb{Z}_p^*, \times_p)$ is a group.

(ii) $(\mathbb{Z}_p^*, \times_p)$ is a group whenever p is a prime number.

(iii) $(\mathbb{Z}_p^*, \times_p)$ is a group provided that p is a prime number.

(iv) p is a prime number only if $(\mathbb{Z}_p^*, \times_p)$ is a group.

(c) There is no definitively right or wrong answer as to which of (i)–(iv) in part (b) are good ways to state the theorem, but a reasonable answer is that (i)–(iii) are good ways, and (iv) is not, as it is less easy to understand.

Solution to Exercise B146

(a) The theorem can be rewritten as follows.

If n is an integer with $n \geq 2$, then the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n and is generated by the integer 1.

(b) The hypothesis is

- n is an integer with $n \geq 2$.

(Alternatively, you can regard the theorem as having two hypotheses:

- n is an integer,
- $n \geq 2$.)

The conclusions are

- the group $(\mathbb{Z}_n, +_n)$ is a cyclic group of order n,
- the group $(\mathbb{Z}_n, +_n)$ is generated by the integer 1.

Solution to Exercise B147

(a) The theorem can be written as

If G is a cyclic group, then G is abelian.

or

If a group is cyclic, then it is abelian.

(b) The converse can be stated as

If G is an abelian group, then G is cyclic.

or

If a group is abelian, then it is cyclic.

or

Every abelian group is cyclic.

(c) The converse is false. For example, $S(\square)$ is an abelian group that is not cyclic.

Solution to Exercise B148

(a) Statements 1, 3 and 6 are correct versions of the theorem.

(Statements 2 and 5 state the converse of the theorem, as mentioned in the solution to part (c) below, and statement 4 claims that in a group of even order *every* element has order 2, which is not what the original theorem claims.)

(b) There is no definitively right or wrong answer to this part, but a reasonable answer is that statements 1 and 6 are good ways to state the

theorem, and statement 3 is not, as it is less easy to understand.

(c) Statements 2 and 5 state the converse of the theorem.

(d) The converse is true, because the order of an element of a group divides the order of the group, by Corollary B69 to Lagrange's Theorem, so a group that contains an element of order 2 must have an order that is a multiple of 2.

Solution to Exercise B149

(a) Lemma B42 can be rephrased as an implication as follows.

> If m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$ and m is a factor of n, then m has order n/m.

The hypotheses are

- m is a non-zero element of the group $(\mathbb{Z}_n, +_n)$,
- m is a factor of n.

The conclusion is

- m has order n/m.

(Alternatively Lemma B42 can be regarded as having three hypotheses, as follows:

- m is an element of the group $(\mathbb{Z}_n, +_n)$,
- m is non-zero,
- m is a factor of n.

However, notice that if an element m of $(\mathbb{Z}_n, +_n)$ satisfies the hypothesis 'm is a factor of n', then it must also satisfy the hypothesis 'm is non-zero'. So in fact the hypothesis 'm is non-zero' in Lemma B42 is not needed: the word 'non-zero' could be omitted from the statement of the lemma. It is included for convenience and clarity: it makes it immediately clear that the lemma applies only to non-zero elements of $(\mathbb{Z}_n, +_n)$.)

(b) Statements 1 and 3 are correct versions of Lemma B42, and statement 2 is incorrect.

(Statement 2 has 'm has order n/m' as a hypothesis and 'm is a factor of n' as a conclusion; they should be the other way round.)

Solution to Exercise B150

(a) The 'if' part of the theorem can be rephrased as an implication as

> If G is a finite group of order n and G contains an element of order n, then G is cyclic,

or slightly more concisely as

> If G is a finite group of order n that contains an element of order n, then G is cyclic.

The hypotheses are

- G is a finite group of order n,
- G contains an element of order n.

The conclusion is

- G is cyclic.

(b) The 'only if' part of the theorem can be rephrased as an implication as

> If G is a finite group of order n and G is cyclic, then G contains an element of order n,

or slightly more concisely as

> If G is a finite cyclic group of order n, then G contains an element of order n.

The hypotheses are

- G is a finite group of order n,
- G is cyclic.

The conclusion is

- G contains an element of order n.

Solution to Exercise B151

(a) The 'if' part is as follows.

> If $m \in \mathbb{Z}_n$ and m is coprime to n, then m is a generator of the group $(\mathbb{Z}_n, +_n)$.

The 'only if' part is as follows.

> If $m \in \mathbb{Z}_n$ and m is a generator of the group $(\mathbb{Z}_n, +_n)$, then m is coprime to n.

(b) For the 'if' part, the hypotheses are

- $m \in \mathbb{Z}_n$,
- m is coprime to n.

The conclusion is

- m is a generator of the group $(\mathbb{Z}_n, +_n)$.

(c) For the 'only if' part, the hypotheses are

- $m \in \mathbb{Z}_n$,
- m is a generator of the group $(\mathbb{Z}_n, +_n)$.

The conclusion is

- m is coprime to n.

Solution to Exercise B152

The theorem can be written as:

> If H is a subgroup of a cyclic group, then H is cyclic.

The contrapositive is:

> If H is not cyclic, then H is not a subgroup of a cyclic group.

It can be stated more clearly as:

> If a group is not cyclic, then it is not a subgroup of a cyclic group.

(It is possible to write the theorem in the form 'If ..., then ...' in a different way, and hence obtain its contrapositive in a different form. The theorem can alternatively be written as:

> If G is a cyclic group, then every subgroup of G is cyclic.

The contrapositive of this statement is:

> If it is not the case that every subgroup of G is cyclic, then G is not a cyclic group.

This can be stated more clearly as:

> If a group G has a non-cyclic subgroup, then G is not a cyclic group.

Different ways of writing a theorem and its contrapositive can be useful in different situations.)

Solution to Exercise B153

Suppose that

$$a^2 = a.$$

Composing both sides on the left with a^{-1} gives

$$a^{-1}(a^2) = a^{-1}a.$$

Therefore

$$(a^{-1}a)a = a^{-1}a \quad \text{(by axiom G2, associativity)},$$

so

$$ea = e \quad \text{(by axiom G4, inverses)},$$

and hence

$$a = e \quad \text{(by axiom G3, identity)},$$

as required.

(Note that we could equally well have composed both sides on the *right* with a^{-1} here.)

Solution to Exercise B154

Suppose that

$$gh = e.$$

Composing both sides on the left with g^{-1} gives

$$g^{-1}(gh) = g^{-1}e.$$

Therefore

$$(g^{-1}g)h = g^{-1}e \quad \text{(by axiom G2, associativity)},$$

so

$$eh = g^{-1}e \quad \text{(by axiom G4, inverses)},$$

and hence

$$h = g^{-1} \quad \text{(by axiom G3, identity)},$$

as required.

Solution to Exercise B155

Suppose that

$$a^2 = a.$$

By axiom G3 (identity), this equation can be written as

$$aa = ae,$$

so, by the Left Cancellation Law,

$$a = e,$$

as required.

(Alternatively, we could have written the equation as $aa = ea$ and used the Right Cancellation Law.)

Solution to Exercise B156

Suppose that

$$gh = e.$$

By axiom G4 (inverses), this equation can be written as

$$gh = gg^{-1},$$

so, by the Left Cancellation Law,

$$h = g^{-1},$$

as required.

Solution to Exercise B157

Suppose that

$$abc = e.$$

Composing both sides on the left with a^{-1} gives

$$a^{-1}abc = a^{-1}e,$$

so

$$bc = a^{-1}.$$

Now composing both sides on the right with a gives

$$bca = a^{-1}a,$$

so

$$bca = e,$$

as required.

Solution to Exercise B158

Suppose that x and y commute. Then

$$xy = yx.$$

Composing both sides on the right with x^{-1} gives

$$xyx^{-1} = yxx^{-1},$$

that is,

$$xyx^{-1} = ye,$$

so

$$y = xyx^{-1},$$

as required.

(We compose on the *right* here because that gives xyx^{-1} on the left-hand side of the equation, which is the expression that we are trying to prove is equal to y. If instead we compose on the *left* with x^{-1}, then we obtain

$$x^{-1}xy = x^{-1}yx,$$

and hence

$$y = x^{-1}yx,$$

which is a different expression for y. This expression is also correct, but it is not the one we were asked to prove.)

Solution to Exercise B159

Two different proofs are given.

Proof 1

Since $(xy)^{-1}$ is the inverse of xy, we have

$$xy(xy)^{-1} = e.$$

Composing both sides with x^{-1} on the left gives

$$x^{-1}xy(xy)^{-1} = x^{-1}e,$$

that is,

$$y(xy)^{-1} = x^{-1}.$$

Now composing both sides with y^{-1} on the left gives

$$y^{-1}y(xy)^{-1} = y^{-1}x^{-1},$$

that is,

$$(xy)^{-1} = y^{-1}x^{-1},$$

as required.

Proof 2

We show that $y^{-1}x^{-1}$ is an inverse of xy. To do that, we have to show that

$$(xy)(y^{-1}x^{-1}) = e = (y^{-1}x^{-1})(xy).$$

Now

$$\begin{aligned}(xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1}\\ &= xex^{-1}\\ &= xx^{-1}\\ &= e,\end{aligned}$$

and

$$\begin{aligned}(y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}x)y \\ &= y^{-1}ey \\ &= y^{-1}y \\ &= e,\end{aligned}$$

so $y^{-1}x^{-1}$ is an inverse of xy. Hence, since every group element has a unique inverse, $y^{-1}x^{-1}$ is *the* inverse of xy; that is,

$$(xy)^{-1} = y^{-1}x^{-1}.$$

(This is the proof that you saw in Unit B1.)

Solution to Exercise B160

Two different proofs are given. The second uses Proposition B14.

Proof 1

Let g and h be any elements of G. We have to show that $gh = hg$.

Every element of G is self-inverse, so $gg = e$, $hh = e$ and

$$(gh)(gh) = e.$$

Composing both sides of the last equation on the left with g and on the right with h gives

$$g(gh)(gh)h = gh,$$

that is,

$$(gg)hg(hh) = gh,$$

which gives

$$ehge = gh.$$

Hence

$$hg = gh.$$

Thus G is abelian.

Proof 2

Let g and h be any elements of G. We have to show that $gh = hg$.

Every element of G is self-inverse, so $g^{-1} = g$, $h^{-1} = h$ and

$$(gh)^{-1} = gh.$$

By Proposition B14, we also have

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Thus

$$gh = h^{-1}g^{-1}.$$

Therefore, since $g^{-1} = g$ and $h^{-1} = h$,

$$gh = hg.$$

Thus G is abelian.

Solution to Exercise B161

Let $P(n)$ be the statement

$$(x^n)^{-1} = (x^{-1})^n.$$

Then $P(1)$ is true, because the equation

$$(x^1)^{-1} = (x^{-1})^1$$

is equivalent to the equation

$$x^{-1} = x^{-1}.$$

Now let $k \geq 1$ and assume that $P(k)$ is true; that is,

$$(x^k)^{-1} = (x^{-1})^k.$$

We want to deduce that $P(k+1)$ is true, that is,

$$(x^{k+1})^{-1} = (x^{-1})^{k+1}.$$

Now

$$\begin{aligned}(x^{-1})^{k+1} &= (x^{-1})^k x^{-1} \\ &= (x^k)^{-1}x^{-1} \quad \text{(by } P(k)\text{)} \\ &= (xx^k)^{-1} \quad \text{(by Proposition B14)} \\ &= (x^{k+1})^{-1}.\end{aligned}$$

Hence $P(k+1)$ is true.

Thus $P(k) \implies P(k+1)$ for all $k \geq 1$. Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for all $n \in \mathbb{N}$.

Solution to Exercise B162

We know from Theorem B81 that $H \cap K$ is a subgroup of G, so $H \cap K$ is a group. Hence to prove that $H \cap K$ is a subgroup of H we just need to check that $H \cap K$ is a subset of H. This is true simply by the definition of $H \cap K$, so the stated result follows.

Solution to Exercise B163

We give a counterexample to the statement.

Let $G = S(\square)$, and take both H and K to be equal to G. Then H and K are subgroups of G and $H \cup K = G$, so $H \cup K$ is a subgroup of G. This counterexample shows that the given statement is not true.

(We could have taken G to be any group at all here, and there are also many other possibilities for H and K: we could have taken them both to be the trivial subgroup, for example, or we could have taken them to be any two equal subgroups.)

Solution to Exercise B164

We give a counterexample to the statement.

Let

$$G = S(\square),$$
$$H = \langle a \rangle = \{e, a, b, c\},$$
$$K = \langle b \rangle = \{e, b\}.$$

Then H and K are distinct non-trivial proper subgroups of G. Also $H \cup K = H$, so $H \cup K$ is a subgroup of G. This counterexample shows that the given statement is false.

(We could have taken H and K to be any distinct non-trivial proper subgroups of a group G such that one of H and K is a subset of the other. Another such counterexample is obtained by taking G to be the cyclic group $(\mathbb{Z}_8, +_8)$ with $H = \langle 2 \rangle = \{0, 2, 4, 6\}$ and $K = \langle 4 \rangle = \{0, 4\}$.)

Solution to Exercise B165

We check that the three subgroup properties hold.

SG1 Let g and h be elements of $\langle x \rangle$. Then $g = x^s$ and $h = x^t$ for some integers s and t. So

$$gh = x^s x^t = x^{s+t}.$$

Since $s + t \in \mathbb{Z}$, this shows that gh can be written as a power of x, so $gh \in \langle x \rangle$.

SG2 The identity element e of G can be written as $e = x^0$, so it is in $\langle x \rangle$.

SG3 Let g be any element of $\langle x \rangle$. Then $g = x^s$ for some integer s. Now

$$\begin{aligned} g^{-1} &= (x^s)^{-1} \\ &= x^{-s} \quad \text{(by one of the index laws).} \end{aligned}$$

Since $-s \in \mathbb{Z}$, this shows that g^{-1} can be written as a power of x, so $g^{-1} \in \langle x \rangle$.

Since all three subgroup properties hold, $\langle x \rangle$ is a subgroup of G.

Solution to Exercise B166

We know that K is a subgroup of H, so K is a group. Hence to prove that K is a subgroup of G we just need to check that it is a subset of G. This is true because K is a subset of H and H is a subset of G. Hence K is a subgroup of G.

Solution to Exercise B167

Let G be an abelian group, and let H be a subgroup of G.

Let $x, y \in H$. Then $x, y \in G$ since H is a subgroup of G. Since G is abelian, it follows that $xy = yx$. Thus H is abelian, as required.

Solution to Exercise B168

Let the order of H and K be p, where p is prime. By Theorem B81, the set $H \cap K$ is a subgroup of G. It is also a subset of each of H and K, so it is a subgroup of each of H and K. Hence, by Lagrange's Theorem, its order divides p, so it is either 1 or p. If it is p, then $H \cap K$ is a subgroup of H that has the same order as H, so $H \cap K = H$, and similarly $H \cap K = K$. But this is impossible since $H \neq K$. Hence the order of $H \cap K$ is 1, and therefore, since $H \cap K$ is a subgroup, $H \cap K = \{e\}$.

Solution to Exercise B169

Let the orders of H and K be p and q, respectively, where p and q are coprime. By Theorem B81, the set $H \cap K$ is a subgroup of G. It is also a subset of each of H and K, so it is a subgroup of each of H and K. Hence, by Lagrange's Theorem, its order divides p and q. Since p and q are coprime, their only positive common factor is 1, so the order of $H \cap K$ is 1. Therefore, since $H \cap K$ is a subgroup, $H \cap K = \{e\}$.

Solution to Exercise B170

Attempt 3
This attempted proof is incorrect. It gives an *example* of a group of even order that contains an element of order 2, but to prove the theorem we have to prove that *every* group of even order contains an element of order 2.

(This kind of 'proof' is known to mathematics tutors as a 'proof by example'; this is not a valid method of proof!)

Attempt 4
This attempted proof is also incorrect. It is a correct proof of the following statement:

> A group that contains an element of order 2 has even order.

This is the *converse* of the theorem to be proved. Unfortunately the fact that the converse of a statement is true tells us nothing about the truth of the original statement.

(The solution to Worked Exercise B56, Attempt 2, gives another way of expressing the converse – that way is the contrapositive of the statement above.)

Attempt 5
This attempted proof is correct. It correctly proves the contrapositive of the theorem to be proved, and the contrapositive is equivalent to the theorem.

(However, the proof would have been clearer if it had started by saying that it was going to prove the contrapositive and had then stated the contrapositive.)

Attempt 6
This attempted proof is incorrect. The problem occurs in the step 'Then there is no element x of G that satisfies the equation $x^2 = e$.' This is not a correct deduction, because even if a group does not contain an element of order 2, there is still an element x of G that satisfies the equation $x^2 = e$, namely the identity element e.

(Saying that an element x has order 2 is not *equivalent* to saying that $x^2 = e$. If an element x has order 2, then it follows that $x^2 = e$, but if an element x satisfies $x^2 = e$ then it does not follow that it has order 2, as x could be e, which has order 1.)

Solution to Exercise B171

(a) The problem is that to show that the order of ba is n, we have to show not only that $(ba)^n = e$, but also that there is no natural number k smaller than n such that $(ba)^k = e$.

(b) We can fix the proof by adding the following immediately before the sentence 'Hence ba also has order n.'

> Now suppose that there is a natural number k smaller than n such that
>
> $$(ba)^k = e.$$
>
> Then, by an argument similar to the one above, it follows that
>
> $$(ab)^k = e.$$
>
> But this contradicts the fact that the order of ab is n. So there is no such natural number k.

Alternatively, we can exploit the fact that the elements a and b in the original statement are interchangeable, and replace the sentence 'Hence ba also has order n.' by the following.

> Let the order of ba be m. Then the argument above shows that $m \leq n$. By the same argument, with the roles of a and b interchanged, it follows that the order of ab is at most m; that is, $n \leq m$.
>
> Since $m \leq n$ and $n \leq m$, we have $m = n$.

There are other possibilities for fixing the proof, apart from the two suggestions above.